Vol 1, Spring 2010

SCIENTIA

Undergraduate Research Journal for the Sciences
University of Notre Dame

Notre Dame Science

Inside: The Effect of Urbanization on Bird Foraging at Notre Dame

A Letter From Dean Crawford

Research is indisputably the most important component of scientific education. In addition to the valuable discoveries students of science make by doing research, it is in making those discoveries that they learn how to ask and probe big questions of our day and be scientists. For a scientist, the main emphasis falls on creating knowledge through research and investigation, rather than collecting passed-down information.

Nevertheless, given that research is not a goal in itself, but rather a means to an end, it is essential that the created knowledge be available not only to the researcher and other members of his or her lab but to other members of the scientific community and to those who have the means to translate it into usable products. It is by publishing their findings that scientists opens channels of communication to colleagues in other departments, colleges, universities, and even countries, which enables collaboration on a global scale. And it is by publishing their findings that they are able to disseminate their ideas to the world for others to confirm, build upon, or advance. Research findings may lead to a cure for a disease, a solution to an environmental program, or they may improve upon our understanding of a fundamental principle.

At Notre Dame, we recognize the importance of undergraduate research, and the College of Science makes every effort to provide its students with research opportunities from the very beginning of their freshman year. Since the winter of 2009, the student-run online publication of *Scientia* has provided a forum for our students to disseminate their discoveries while getting practical experience with scientific writing. Those students involved with the publication of *Scientia* learn about peer review, publication, and editing. It is my pleasure to introduce the inaugural printed publication of this journal. I am filled with pride and inspiration when I consider the accomplishments of our talented students. May they inspire you as well!

Yours in Notre Dame,

Gregory P. Crawford,
William K. Warren Foundation Dean of the College of Science

Editorial Board 2009-2010

Acknowledgments: The Scientia editorial board expresses its gratitude for the dedication and guidance of our faculty advisor, Dominic Chaloner, Ph.D. Scientia represents exclusively undergraduate research, and we are sincerely thankful to the students who submit their work. We would also like to thank Marissa Runkle for helping us through the publication process. Finally, we would like to recognize the College of Science, Balfour Program, and ND Journal of Formal Logic for their financial support.

From the Editors

If the doors of perception were cleansed everything would appear to man as it is, infinite.

–William Blake

Scientia is proud to present its first print publication, showcasing outstanding undergraduate scientific research at Notre Dame.

The goals of *Scientia* are threefold: first, to recognize and encourage high-quality undergraduate research. The seven papers published in this volume represent commendable persistence and bold thinking. They were selected for their demonstration of excellence in data, novelty, and quality.

Second, to provide a forum through which students can gain experience of the essential skills of writing and reviewing to fulfill their future professional goals. *Scientia'*s twenty-one member editorial board, comprising of students from every department and grade level in the College, has reviewed and edited over twenty papers in our first year. We hope to double this number during the upcoming year.

Finally, *Scientia* strives to contribute to the advancement and cohesiveness of Notre Dame's scientific community of which undergraduates are part. *Scientia* is Latin for "knowledge," and our publication serves not only to display but also to encourage the collective pursuit of truth that first takes form at the undergraduate level. To this end, we celebrate curiosity-driven research as a means to further knowledge for, as Albert Einstein said, while "*knowledge is limited to all we now know and understand… imagination embraces the entire world, and all there ever will be to know and understand*."

We are grateful to everyone who has contributed to this first installment of *Scientia*, and are enormously glad to be able to share the product of their hard work with our readership.

In Notre Dame,

Matt Reagor and Melissa Harintho

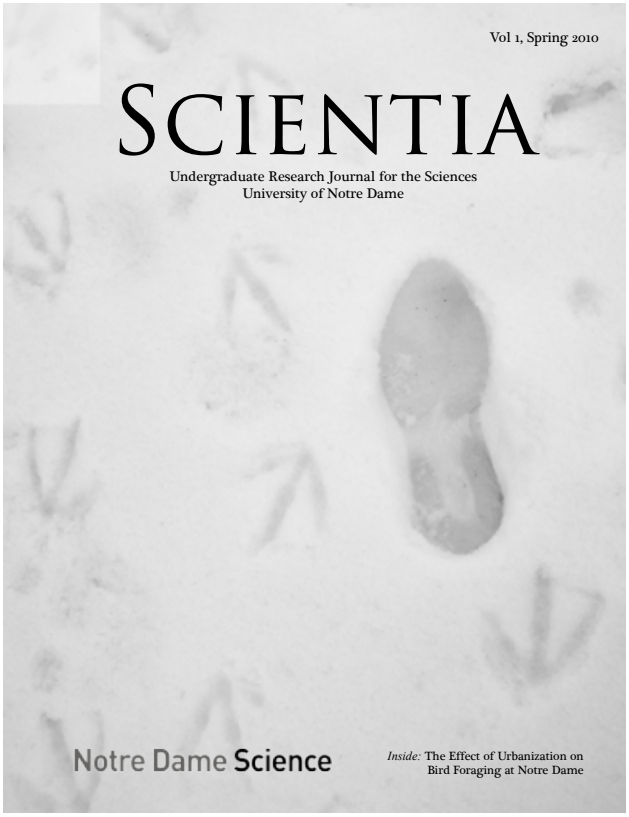
Contents

News

Math

Health

Biology



Physics

Cover: Foraging studies reveal Notre Dame's potential impact on the local ecosystem -*Chan & McCormack. p. 31*

Hope for Haiti:

Eradication of Lymphatic Filariasis in the Midst of a Disaster

By: Kirsten Adam

The people of Haiti face a very small problem. This problem is small in size only, not in scope. The minuscule parasites that lead to a disease called lymphatic filariasis are a disaster that preceded January's earthquake, and they continue to impact the lives of Haitians day after day. As Haitians struggle to pick up the pieces from an outside disaster, many also wage an internal war.

Lymphatic filariasis (LF) is a mosquito-borne, debilitating disease caused by parasitic worms that attack the lymphatic system and circulate in the blood. The disease results in lymphedema and elephantiasis. Elephantiasis, or the uncontrollable swelling of the lower limbs or genitals, leads to further infections, immobilization, and social isolation.

Approximately 10% of the population of Haiti suffers from LF, and in some hyper-endemic areas that percentage approaches 50%. Without treatment, virtually the entire population of Haiti is at risk for contracting the disease.

In 1997, the World Health Assembly declared LF as one of only six eliminable infectious diseases. To date, smallpox is the only infectious disease that has been eradicated by an implemented public health program. Eliminating a disease like LF would be a groundbreaking accomplishment for the public health sector.

Above: The view from Residence Filariose. (Photo: Ralph Pennino)

Soon after this 1997 announcement, the University of Notre Dame shifted its focus from public health research to implementation of a program for disease elimination. Notre Dame Haiti Program coordinator, Sarah Craig, says, "Notre Dame was really a catalyst for getting a treatment program going. But we had no idea of the amount of money that it would actually take."

A 1999 grant from the Bill & Melinda Gates Foundation, and a second grant in 2006, allowed the Notre Dame and sister health organizations to put a mass-treatment program into action. The first distribution of 200,000 treatments took place in 2000. The number of treatments has steadily increased since then.

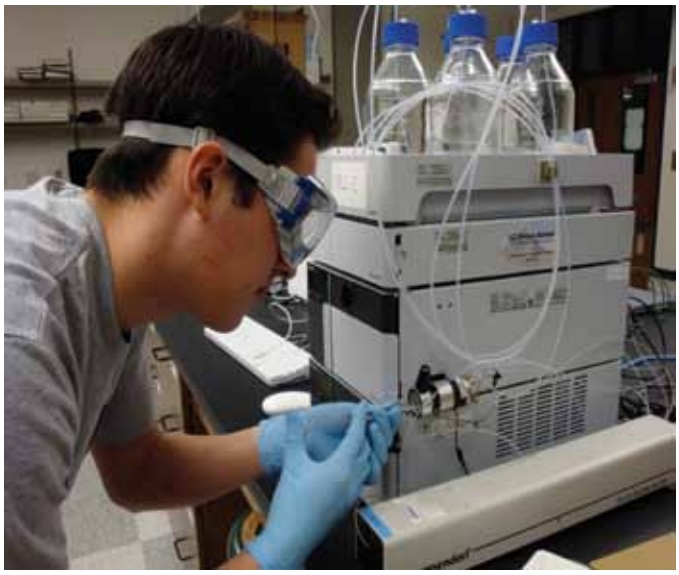
Treatments may be administered annually in the form of diethylcarbamazine (DEC) and albendazole tablets, called Mass Drug Administration (MDA). A secondary treatment method is the distribution of treated salt. The salt is cofortified with an antiparasitic agent and iodine, to

Above: What remained of the Church of Ste. Rose of Lima several days after the earthquake. The church is home parish to ND Haiti Program director, Fr. Tom Streit, for serveral months out of the year. (Photo : Ralph Pennino)

treat both LF and iodine deficiency disease.

The catastrophic earthquake that occurred in January severely damaged the ability of outside relief programs to provide the treatments necessary to combat the spread of the disease. In the shadow of the disaster, the ND Haiti Program and its sister programs are once again undergoing a major shift in their approach to relief for Haiti. The primary focus must now center on providing urgent needs in the aftermath of disaster- food, water, shelter, and medical care.

It is estimated that 80-90% of the buildings in Leogane collapsed in the earthquake. Leogane is one of the areas in Haiti most severely affected by LF. It is here that the fight to eliminate LF began with the Haitian ministry of Public Health and Population, the Hopital Sainte Croix, and the US Centers for Disease and Control Prevention. The ND Haiti Program residence, Residence Filariose, remained intact after the earthquake. From here, ND Haiti Program and its partners immediately began coordinating relief efforts.



Doctors and volunteers have flown in to help, doing as well as they can with a lack of supplies and transportation. "Getting supplies in has been crucial," says Craig, "So far we have flown in over 3½ tons of food, 250 tents, and many reverse osmosis machines for purifying water."

Getting supplies to Haiti has not been easy. The only airplanes into Leogane have landed on a country-road turned into a makeshift airstrip. Pick-up trucks for supplies double up as ambulances. Logan Anderson, manager of finances for the Haiti program, says, "The Notre Dame program lost three cars in the earthquake. It may be several months before we can replace even one of them."

Above: Regan McGann '12 checks the level of a sample in a dilution flask. Left: Marco Magallon '12 loads a sample for testing. (Photos: Kirsten Adam)

In the meantime, relief workers have been doing what they can to make up for what they lack. Doctors have been forced to perform surgeries and amputations with little more than a kitchen knife. Craig says, "A temporary hospital was set up soon after the earthquake. Several Notre Dame alumni came to help out. So far the hospital has treated over 7,000 patients and performed over 250 surgeries."

Safe on campus at Notre Dame, it is hard to imagine the extent of the damage in Haiti. However, this damage is exactly what those involved the Haiti Program do their best to remember every day. Coordinating efforts from hundreds of miles away keeps efforts in the disaster area running smoothly. Craig says, "What undergraduate students don't always get to see is a public health program in operation- the intensity of administration it takes, and the importance of collaboration between science and business."

Several undergraduate students working in a Notre Dame lab have already started to appreciate the impact that management and service can make, even from a distance. Undergraduates working in a chemistry lab meet in Jordan Hall of Science once or twice a week, surrounded by zip-loc bags full of salt

and dilution flasks with carefully measured samples. One of the undergraduate lab volunteers, Marco Magallon, explains, "What we do here is basically verify the numbers that chemists in Haiti get. We measure the level of DEC in the salt treatment to make sure that each batch of fortified salt is safe before it gets to consumers."

Another undergraduate lab volunteer, Regan McGann, says, "At first, I wondered if we were going to keep up with our work here. It somehow seemed irrelevant in the face of other larger disasters. But with these conditions, a disease like LF can spread even more, so it's important to keep going."

The goal originally set for 2010 was to increase the number of MDA treatments to 5.2 million. This increase is being reevaluated in light of the current difficulties the program faces, but there are still plans underway to begin some level of treatment distribution in May.

Brennan Bollman, 2009 valedictorian, worked for the Haiti Program during her time at Notre Dame. In early March of this year, Bollman made the trip to Haiti to help in the relief efforts. Taking time off from Harvard Medical School, she is acting as ND Haiti Program Response Manager.

Bollman says, "This is the moment for everyone who cares about Haiti to work together in allowing Haitians to reimagine their country. Not only did I feel personally called to be involved in this, but I also want to contribute to the way Notre Dame deepens its engagement."

McGann also sees the potential for good to come of the disaster in Haiti. She says, "The positive thing about the earthquake is the attention it is bringing to Haiti. Hopefully, with this attention and aid Haiti is receiving, we can bring about changes that are longer lasting and deeper than we could have made before.

For more information or to make a donation to the current relief efforts, visit online at:

http://haitidisaster.nd.edu.

Changing Perspectives: The Science of Psychology

By: Danielle Rush

If one were to ask a student which major offered at the University of Notre Dame would best foster a deeper understanding of the physiological explanations for natural human tendencies, it is unlikely that Psychology would be the first answer. However, the College of Science is not the only department to emphasize the importance of developing a strong foundation in the sciences. Several undergraduate majors within the College of Arts and Letters, including Psychology, have recently been attempting to answer the question "Why are we the way we are?"

Michelle Wirth, Assistant Professor of the Department of Psychology, offers students the intellectual challenge of core science classes in an interactive and personable environment. Her Biopsychology class introduces students to topics commonly overlooked in general science electives, such as physiological psychology and behavioral endocrinology. The enthusiasm with which her students respond to her method of teaching is palpable. Jena Doom, a junior Arts and Letters Pre-Professional/Psychology major, admires the ability of Professor Wirth to instruct on the effect that the mechanisms of biology have on our daily lives: "the tiny details we are taught in a science course are applied in real world situations, which have been incredible to discover."

Many students even prefer the interactive and detail-oriented approach of psychology to science over the broad range of simplified topics covered in giant lecture halls in General Biology or Chemistry. Heather Hyland, also a junior Arts and Letters Pre-Professional/Psychology major, firmly believes that the Psychology component of her major has allowed her to grasp the mechanistic explanation behind behavioral norms in all humans, an understanding that is a critical part of her future career path. She is confident that by understanding how people think and behave, she will be a much more effective and empathetic doctor. An education in Psychology has given her a clear advantage in her chosen field, one that is not afforded to students' whose education is limited to that of science classes that merely brush over critical topics of emotion, motivation, hormones and behavior. Heather states:

"While it is important to be able to treat patients

based on specific problems from a physiological standpoint, it is also important to be able to understand why people think and behave in certain ways. My psychology classes taught me the importance of treating the whole patient by also addressing any problems the patient might have from a psychological standpoint."

While it is informative to learn specific details of the physiology that drives psychological patterns, lecture and discussion cannot replace the importance of hands-on activities in solidifying knowledge gained in the classroom. Another student, Kathy Poplowski, found that the sheep brain dissection she conducted as a component of her Biopsychology class strengthened her foundation in both neuroanatomy and neurophysiology. Kathy notes that "the research information offers another dimension to the subject" as opposed to simply glazing over factual content. "Psychology adds a personal aspect to science; it shows how research is affecting peoples' lives daily."

In an effort to inform the student body of the modern research being conducted in the field of psychology and its application to society, the Psychology Club at the University of Notre Dame is sponsoring "Brain Awareness Week" from March 15 through March 20, 2010. The goal of the weeklong program is to provide guests with the opportunity to explore their own ability to form strategies and test their understanding of paradigms such as the argument of dualism or parallelism, involving cognitive science, education, metaphysics and philosophy.

While philosophy, education and psychology may not be the first areas of study that come to mind with mention of the word "brain", there is no denying that the College of Arts and Letters has expanded its emphasis from an analysis of select individuals and their achievements to a physiological approach as to why those individuals behaved and responded in the way that they did to both internal and external stimuli. So, before you facetiously critique your friend for selecting his or her respective College of Arts and Letters major, think again. Your friend just might be better equipped for real world situations than you are.

EVENTS:

Coverage of lectures, discussions, and events held in conjunction with the Notre Dame College of Science

Blessed Are The Geeks

By: Martha Karam

This year Notre Dame hosted its "Geek Week" during the last week of February for every student on campus who is a Science, Math or Engineering major. The purpose of the weeklong celebration was to bring together all the "geeky" majors.

"Geek Week's" success this year far exceeded expectations of the hosting clubs and even the participants. Keith Nord, a Sophomore Engineering major, said, "this year they really stepped up the prizes- a $75 Best Buy gift card for first and $50 for second." Nord competed in the three-hour long Mario Kart tournament hosted by the College of Engineering that Senior Emmanuel Bello-Ogunu won. Nord added, "it was a good time, I was surprised to see so many people there to play a game made thirteen years ago."

Other events held for "Geek Week" also had an unexpectedly high attendance. Sarah Pastorek, Senior President of the Math Club, says that the Sudoku Challenge that her club hosted was "by far our most successful event of the year." The event was held in Jordan Auditorium on Thursday and was expected to host about fifty competitors, but to the surprise and panic of the Math Club nearly one hundred students showed up to compete for the prize of a 4 GB iPod Shuffle.

College of Science students take a break for a picture at the Geek Week dance. (Photo: Paul Baranay)

Jordan Matulis won first place raking in 11 points, or 7 puzzles in half an hour, and took away the grand prize. Second and third place did not leave empty handed- they each one bookstore gift certificates. The incentive of attending the event was Subway cookies, but according to Pastorek, many professors offered bonus points to students who attended.

Also held in Jordan Hall, the Biology Club hosted a dissection night assisted by Valerie Schroeder from the Freimann Life Sciences Center who instructed and displayed diagrams with the various organs and anatomical features of the rats dissected. The event had ten rats with groups of 2-3 students working on each rat. Annette Ruth, president of the Biology Club, said "everyone was very fascinated and excited about the event, and all the participants worked together very well…one of the students mentioned that they had never had the opportunity to do a dissection so they were happy that they had the chance to do so."

The Biology Club also hosted a dance on Friday, February 26th in the Jordan Galleria to usher the end of "Geek Week." The dance's theme was "Beauty and the Geek", and according to Paul Baranay, the Social Commissioner for the Biology Club, the costumes ranged from lab coats and pulled-up pants to tuxes and dinner gowns.

The dance was funded by the Biology Club, but also received a generous grant from Dean Crawford and the College of Science. The dance was not only a way for students to relax right before midterms, but was also a charity event- the recommended donation was a canned good for attending that went to the Center for the Homeless.

Baranay says, "I think the event was a great opportunity for students to mix and mingle with their peers in a more relaxed setting than they usually find in the classroom. A number of the party-goers were also from outside the College of Science, which was very encouraging, as humanities and science majors don't often socialize with each other."

Students of various majors attended the events of "Geek Week" and thus the purpose of the events, to facilitate socializing and learning among students who are normally confined to their major-specific course-work and labs, proved to be an achievement for all of the clubs that made it possible.

College of Science Colloquium

By: Martha Karam

Professor Carlos E.M. Wagner visited Notre Dame on February 24th to speak on "New Physics at the Weak Scale: From Collider Physics to Cosmology." Wagner is a member of the University of Chicago's Physics Department specializing in theoretical physics, elementary particles, and supersymmetric theories. Wagner completed his Ph.D. at the University of Hamburg and conducted a post-doctoral appointment at Purdue before joining U. Chicago.

Wagner's talk began with the four known forces in nature that every freshman must learn but quickly jumped into gritty physics that excited the few in the room capable of understanding. After distinguishing between weak force and strong force, Wagner began to discuss the future of dark matter in the physical world and how scientists can begin to go about locating and measuring dark matter. He also discussed methods for exploring Higgs physics, including the Tevatron and the Large Hadron Collider (LHC).

Recently, in September of 2008, the Tevatron achieved the sensitivity to exclude Higgs by colliding protons and antiprotons and quarks with antiquarks. Despite the technology of the Tevatron, the future of collider physics lies in the LHC. The LHC is the world's largest and highest energy particle accelerator and is located near Geneva and is the world's most expensive scientific experiment to date. Presumably, the LHC will be able to find the Higgs Boson in a matter of years. Wagner and most contemporary physicists believe that over the next decade, the Tevatron will become obsolete and the LHC will reach full development and usage.

The subject of theoretical physics may be over many undergraduates' heads or uninteresting to non-physics students. Thankfully though, an employee of CERN's LHC created a youtube rap video to give Americans a crash-course on the project called "Large Hadron Rap."

The importance of the work that laboratories, such as Argonne National Laboratory in Chicago, are conducting lies in the fact that dark matter makes up most of the matter in the universe. Physicists hypothesize that 73% of the universe is dark matter, 23% is cold dark matter and only 4% is atoms that make up our physical world. Though the $9 billion price tag on the LHC project may be overwhelming, the price is small in comparison to the discovery of 73% of the universe.

The Synthesis of My Journey in Undergraduate Research

By: James Rudloff

Of all the medical advances throughout history, no single discovery has increased the average human lifespan more than the discovery of antibiotics in 1928. Yet, despite humanity's fortune due to antibiotics, the evolutionary capabilities of bacteria and other microorganisms have made novel drug discovery a major concern. Even today within our modern societies, new drug resistant strains of diseases once thought to have been treatable are developing at alarming rates. Though previous scientific research has continuously developed new drugs, these drugs are typically only modified versions of a particular class, not new classes themselves. Between 1962 and 2000, no new significant classes of antibiotics were developed. Considering the significant speed at which bacteria develop resistance, this innovation gap is disturbing. With drug companies turning away from novel antibiotic discovery, the need for developing new classes of antibiotics is dire! Dr. Marvin Miller at Notre Dame and other researchers throughout the world are piloting this effort in novel antibiotic class discovery.

Of all my classes, none had ever challenged me in the way organic chemistry has. Drawn to this unique field and having done well in Dr. Miller's class, I was fortunately able to work out an opportunity to join his lab. Since the fall of 2008, my research has focused on design, synthesis, and testing of a potential novel class of antibiotics. In regards to my overall project, I focus on one "core" structure of molecules that has potential as a backbone for a novel class of antibiotics. By coupling amino acids to this "core" structure, we hope to see biological activity when tested against strains of bacteria. Based on previous research by the Miller group, this particular "core" structure has a great deal of promise. My typical day in lab entails researching past chemistry literature related to my target molecules, applying the chemistry, and performing the necessary reaction to synthesize my target compounds. Following analysis and troubleshooting (if I make a mistake, which is far more common than one might anticipate), we are able to test my target compounds in qualitative, in-house biological assays. With hard work, patience, and the support of the Miller Lab, I hope to have significant results at the end of this upcoming summer.

Of the countless benefits I have been fortunate enough to experience while working in the Miller group, I have appreciated my new opportunities the most. This past summer I worked at Eli Lilly & Company in a competitive nationwide scholarship. During my time both at Notre Dame and Eli Lilly, I have shaken hands some of the most famous scientists and businessmen in America. Though research can be difficult and frustrating, my experiences thus far have been exceptional.

Coming in as a freshman, if you had told me that I was going to engage in undergraduate research at Notre Dame, I would have laughed at you. If you had told me my research discipline would have been the dreaded, feared, vilified organic chemistry, I would have laughed at you twice. Yet, at my current pace I will have completed six semesters of research with Dr. Miller when I graduate in 2011. As I engaged in my classes at Notre Dame, research became evident to me as a new way to expand my interests is science. Research is the ultimate learning experience for a science major; a scientist not only expands his knowledge in his field, but also makes discoveries that no one else in history ever has done. Research in any field is a constant learning experience; we never cease to be students. For these reasons, I anticipate research will become an integral part of my future.

Perspectives: Real-time Tracking of Influenza-like Illness Using the Argus1Online Surveillance System

Charles N. Spear
University of Notre Dame, Pre-Professional Sciences

Influenza, or "the flu" as most people call it, is an infectious disease that most often results in fever, fatigue, and general discomfort for nearly everyone who has been exposed to it. Whether we have experienced the symptoms first-hand or have witnessed outbreaks during various flu seasons, it can be said without hesitation that the role of our public health authorities in containing and preventing influenza among our population is of crucial importance. This is especially so following this past year's recent outbreak of the novel H1N1 virus throughout our global society. Nevertheless, our reliance on health care professionals and research teams to find the cures and vaccines to treat the flu is considered paramount to our global health. However, few people seem to recognize the need for effective and timely infection surveillance amongst clinicians and medical institutions. Implementing an easy-to-use influenza surveillance system designed for rapid and uniform communication between health care professionals and members of the general public would greatly enhance the quality of patient care and the prevention of worldwide pandemics.

This is exactly what Dr. Vincent E. Friedewald realized and intended to pursue in the development of the Argus1 online surveillance system, designed to provide doctors and medical staff with real-time access to individuals presenting with signs and symptoms of influenza. After speaking with Dr. Friedewald about the program and the benefits that would result from computer-assisted surveillance, I was quick to accept the opportunity to help research the development of Argus1. As we continue to improve the system and analyze the results and feedback from its users, my role in this research has given me the opportunity to step outside of traditional laboratory research settings and into situations where I can analyze user and patient feedback in a more direct and clinically-related approach.

The outset of my work involving Argus1 entailed familiarizing myself with current trends and conventional means of clinicians reporting infection. This helped me better understand how our program differed with respect to what other forms of surveillance were being offered. In addition, I researched various types of institutions and situations in which the Argus1 software could potentially benefit its users in terms of tracking increased incidences of influenza as they occur in real-time. Essentially, I took it upon myself to think of novel ideas for the use of such a surveillance system and to determine whether or not they would be practical and effective.

For example, Dr. Friedewald and I had discussed the use of Argus1 in tracking a college university's student population who presented symptoms of influenza during the academic year. Having Argus1 available on a university's website would allow students and faculty to track – in real-time – instances when an outbreak of the flu was reported. From the perspective of public health officials, implementation of such a program would help explain certain modes of transmission and would offer authorities recommendations for containment. Furthermore, we explored the idea of creating an iPhone application that would allow users to conveniently access Argus1 for tracking their particular location or university. These ideas required researching whether or not similar programs already existed for schools around the country and if other forms of influenza surveillance existed to track real-time flu-like symptoms. In sum, this initial part of my research on Argus1 exposed me to the importance of infection control communication and allowed me to educate myself regarding surveillance as a necessary component of infection prevention.

The next step in my research was to become familiarized with the Argus1 program itself. Since the system was designed before I started researching the advantages of the program, I had to learn more about the particular uses of the system so that when it came my turn to evaluate user and patient feedback I would know what was being said. Argus1 allows its users to input reported cases of influenza-like illness (ILI) and the various symptoms associated with it into a vast online database that compiles information from multiple users and sorts it into numerous categories based on demographics, location, etc. It also allows those who input data to observe the trends (in graphical format) associated with a particular symptom or diagnosis among members of the patient population within a particular vicinity. Yet

what separates Argus1 from traditional surveillance programs is that it allows users to view real-time data of those presenting with ILI so that medical staff members can observe up to the minute results on the spread of influenza.

Immediately after medical staff sees a patient that demonstrates symptoms of ILI, they are able to input this record into the Argus1 system. They input patient information regarding the individual's age, onset of symptoms, and the particular signs and indications of ILI. The program gives users a list of possible symptoms to assign to the patient. Based on this information, the program then lists the various diseases or illnesses that are associated with the symptoms presented so that users can narrow down what the cause of a patient's condition may be. In addition, it allows users to observe any trends in the symptoms among patients of a similar demographic or location by giving them access to other individuals entered into Argus1 by other medical staff members. In conclusion, Argus1 was designed as a user-friendly program that required minimal training to understand and fully operate.

Next, I analyzed the Argus1 software to evaluate user feedback in order to determine the program's areas of strength and needs for improvement. This part of the project constituted the bulk of my research as I received the opportunity to witness first-hand the use of the system and to speak directly with its users. Implementation of Argus1 was tested by school nurses of the Laredo Independent School District (LISD) in Laredo, Texas where they inputted data of their students presenting symptoms of ILI. Located in a predominantly Hispanic community, LISD consists of 32 schools ranging from elementary education to high school. For these particular trials, Laredo served as a great place to start in terms of collecting information regarding the flu since the city happens to be right on the border of Mexico, the country where the H1N1 virus originated. Over the course of its implementation (approximately 4 months) LISD encountered over one thousand cases of students with flu-like symptoms, which essentially translates to over one thousand separate data entries into the Argus1 surveillance system. With so many data entries we were able to organize all of this information to determine the most common symptoms, the most likely causes, times when ILI occurred most frequently, schools that received the greatest number of cases, and the particular demographic that was most often associated with having ILI. Since the software itself compiled these trends for us, it was my responsibility to evaluate subjective data from the users of the program and to hear their insights into the use and potential of Argus1.

In order to accomplish this Dr. Friedewald had me develop and conduct a survey among 28 of the LISD registered nurses. This proved quite challenging as I was forced to come up with survey questions that would elicit unbiased responses and any insights from the nurses that they gained throughout the program's use. However, after multiple drafts and with the help of some nursing colleagues at Texas A&M International University we were able to create an extensive survey that covered all bases in terms of a school nurse's opinion towards Argus1 and influenza surveillance. Once this was completed, it was my job to conduct one-on-one interviews with each of the school nurses at their respective schools about their particular experience with the system. For instance, we attempted to understand the user's experience in receiving training to learn to use the program, as well as whether he or she felt that more help should have been given to fully master ILI tracking. In addition, we asked nurses to describe any technical or day-to-day difficulties encountered that prevented them from entering data into the program.

One common problem that seemed to concern multiple users was incidental duplication of cases in which patient data was entered incorrectly, while the program would not allow for the user to make changes. This obviously has significant effects on the outcome of providing health professionals with an accurate picture of ILI surveillance. Thus, nursing insights proved to be quite valuable. Another question gauged nurses' attitudes towards the potential that a system such as Argus1 would have on school nursing and public health. For the most part, nearly all the LISD nurses felt that a program geared towards real-time detection of influenza had positive nursing implications and would likely raise more awareness on current medical issues.

Overall, this part of our study allowed me to engage in a different form of active research that afforded me the opportunity to step outside of the laboratory and into a clinical setting where I conducted extensive interviews to help improve our surveillance program. Furthermore, this allowed me to partake in a more subjective component of the research process as opposed to simply collecting objective data to be put in miscellaneous graphs and tables. Since we have yet to fully evaluate the results of the Argus1 project, we still remain in the process of publishing our report to be reviewed by various journals, including the American Journal of Cardiology and the American Journal of Nursing. My research has

also given me valuable insight into the process of writing a publishable research paper. In determining how to structure our report and deciding what exactly should be included, I spent time reviewing previous publications of articles that fell under the same categories of "surveillance" and "communications." After reading multiple papers and performing literature reviews on similar infection control systems, we were able to better discern what would make our research report more effective upon reading and more journal-ready.

Without question, my time spent researching influenza surveillance has been beneficial in developing my future career as a scientist and health care professional. I have no hesitation about the positive outcomes that the Argus1 surveillance system will bring towards infection prevention and the tracking of ILI. The use of a program at the fingertips of health professionals which allows access to real-time patient surveillance information has many positive implications on public health and infection control that would be of great benefit during times of flu seasons and pandemics involving infectious diseases. As a global society, we must make it a priority to continue to pursue active research in developing surveillance programs for infectious diseases, since the advantages to such a system in promoting public health are virtually limitless.

I would like to extend my many thanks to Dr. Vincent Friedewald who allowed me to join in on the Argus1 project and has guided me through this research process while giving me all the help I could ask for. In addition, I would also like to recognize Patricia Keck of the Laredo Independent School System and the rest of the nursing staff at LISD for their support and guidance throughout my research.

The Effect of Notre Dame Football on American Catholic Curch Attendance

Talyor Blachley
University of Notre Dame, Department of Mathematics

Abstract

This study examines the effect of the performance of the Notre Dame football team on American Catholic church attendance. Using data taken from the General Social Survey across eleven recent years and the statistical package STATA, I regressed a myriad of variables on Catholic church attendance to explore the effect of Notre Dame football. After determining the relevance of a broad spectrum of inputs, a regression revealed that the success of the Notre Dame football team has a small yet statistically significant positive correlation with American Catholic church attendance.

Introduction

What determines a person's religious involvement? What factors contribute to how often a Catholic attends Mass? Is it a person's age? What about marital status, income, location of residence, or education? Is it a combination of all these and more? These are very difficult questions to answer because there is no one aspect of a person's life which can accurately determine that person's religious involvement in the form of attending Mass.

Undoubtedly, the many complicated aspects of Catholic people's lives combine to effect their decision as to how often to attend Mass. However, something one might not think of when pondering this topic is the effect that the most prominent American Catholic university's football team has on the nation's Catholics. There is a saying that goes: "The second most important person in the Catholic Church is the quarterback of the Notre Dame football team." This study will test that statement. Using econometric techniques, I attempt to determine whether the success of Notre Dame's football team has any discernible effect on Catholic church attendance.

Procedure

The General Social Survey (GSS) conducts periodic surveys of many aspects of Americans' lives [1]. They ask questions ranging from age and marital status to political party affiliation to religious church attendance, and beyond. Their results are compiled in spreadsheets and are available to the public for use in studies such as this. The surveys from 1990, 1991,1993,1994,1996,1998,2000,2002,2004,2006,and 2008 were used in this study. Because these surveys were conducted in the early months of the year, the previous college football season was used in determining the relationship between the success of the football team and Catholic church attendance. For each of the surveys, I used the outsheet function in Stata to convert the data for select variables to an Excel comma delimited spreadsheet. I included in my data set those variables that I thought directly contribute to a random person's religious involvement. I combined all the data into one spreadsheet

and added a variable for Notre Dame football. Since Notre Dame plays different numbers of games from year to year, simply counting the number of wins or losses would not have captured an accurate measure of success for the team. So, I used win percentage to determine a measure of success for the Notre Dame football team.

Survey Year	ND Season	ND W-L-T (pct)	Survey Year	ND Season	ND W-L-T (pct)
1990	1989	12-1-0 (.923)	**2000**	1999	5-7-0 (.417)
1991	1990	9-3-0 (.750)	**2002**	2001	5-6-0 (.454)
1993	1992	10-1-1 (.875)	**2004**	2003	5-7-0 (.417)
1994	1993	11-1-0 (.917)	**2006**	2005	9-3-0 (.750)
1996	1995	9-3-0 (.750)	**2008**	2007	3-9-0 (.250)
1998	1997	7-6-0 (.538)			

Before continuing, the GSS data needed to be checked for errors or impossible outliers. Some entries in the GSS data did not conform to the approved coding entry system as put forth in the GSS Codebook. Since I was unable to determine what these anomalous entries meant, I deleted from consideration all persons with indecipherable answers to any questions. The data was then filtered so that only those people who identified themselves as Roman Catholic were in my data set. After filtering and cleaning the data, my data set included 5,429 surveys to analyze.

All of the variables in the GSS data used a number system; for example a person living in New England would have "1" as the entry in the variable region. However, the meaning of the parameter β would not be clear if the variable region was used in its original form. Therefore, I created dummy variables to use in place of variables, like region, that posed this problem.

After creating all necessary variables, the next step was to determine the relationship between Notre Dame's win percentage and Catholic church attendance. My goal was to use the method of Ordinary Least Squares (OLS) to run the regression

$$\text{attend} = \beta_o + \beta_1(\text{ndwin}) + \beta_2 x_2 + \cdots + \beta_k x_k + u$$

and attempt to interpret the parameters β_i. However, several issues needed to be dealt with before I could proceed. First, could I use the OLS method at all? Did my data conform to the necessary assumptions? A further examination was necessary.

Gauss Markov Assumptions

1) **The dependent variable is linear in the independent variables.** By adding nonlinear functions of those variables where this is not likely to be true, this assumption is accounted for.

2) **The sample is random.** GSS is taken with a random sample.

3) **"Zero conditional mean:" $E[u|x_i] = 0$** It is reasonable to think that the unobservable component of the regression is, on average, zero. Also, information about the independent variables is unlikely to give insight into the unobservable component thereof.

4) **No perfect co-linearity among the independent variables.** By omitting the necessary dummy variables, this will be ensured.

Homoskedasticity

5) Variance$(u|x_i) = \sigma^2$

This assumes that the variance in the unobservable component is constant, given the independent variables. This may not be true, so the method of Feasible General Least Squares (FGLS) will be used.

Another pending question: Which variables best describe a person's religious involvement? This is a difficult question to answer. With the necessary assumptions accounted for, and the data prepared for econometric analysis, I ran several regressions using different combinations of the variables in the table above in an attempt to determine the effect of Notre Dame football on Catholic church attendance. Hopefully the effect of the many aspects of a person's life would help me to understand which are the most important and, in relation to the others, how much the success of the Notre Dame football team influences the nation's Catholics' collective decision as to how often to attend Mass.

Analysis and Results

In order to study the effect of certain variables on some other variable, one must estimate the parameters, β_i, in the equation:

$$y = \beta_o + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_k x_k + u$$

In this case, y is Catholic church attendance. However, one must decide what the independent variables xi should be. To do this, I performed several regressions and interpreted the values of the parameters β_i. First, I simply regressed attend on ndwin, using the equation:

$$\text{attend} = \beta_o + \beta_1 \text{ndwin} + u$$

to gain a preliminary idea of the effect of Notre Dame football on Catholic church attendance. The statistical package Stata was used for the regression analysis, and the above figure is the table of results as calculated by Stata. Before interpreting the parameters, one must understand that the variable ndwin is

Linear regression

Number of obs	5429
F(9, 5419)	45.91
Prob > F	0.0000
R-squared	0.0713
Root MSE	2.4454

attend	Coef.	Robust Std. Err.	t	P>|t|	[95% Conf.	Interval]
ndwin	.5867144	.155339	3.78	0.000	.2821876	.8912412
age	.0386796	.0237549	1.63	0.104	-.0078896	.0852488
sqrtage	-.1768877	.3191077	-0.55	0.579	-.802467	.4486917
widow	-.1363867	.1559837	-0.87	0.382	-.4421775	.1694041
divorc	-.9706306	.1055615	-9.19	0.000	-1.177574	-.7636877
separ	-.563121	.2003857	-2.81	0.005	-.9559575	-.1702844
nevmar	-.5846448	.1005953	-5.81	0.000	-.781852	-.3874377
sibs	.0284537	.0110107	2.58	0.010	.0068683	.0500391
childs	.038628	.0236039	1.64	0.102	-.0076451	.0849011
_cons	3.190043	1.064583	3.00	0.003	1.103033	5.277054

Question: How often do you attend religious services?

Respondent's Answer	Entry in Variable attend
Never	0
Less than once a year	1
About once or twice a year	2
Several times a year	3
About once a month	4
2-3 times a month	5
Nearly every week	6
Every week	7
Several times a week	8

on a unique scale of win percentage, which is defined in [0,1]. Also, the variable attend is a scale, 0-8.

The coefficient β_0 is 3.661426, meaning that, theoretically, if Notre Dame's win percentage is zero, then Catholics' average response to the question is somewhere between "Several times a year" and "About once a month." The coefficient β_1 is 0.5852568. This means that if Notre Dame's win percentage increases by 1, then Catholics' average answer to the question would increase by 0.5852568. However, it will likely be more useful to think of what would happen if Notre Dame's win percentage increased by, for instance, 0.100. In this case, the parameter β_1 means that Catholics' average answer to the question would increase by 0.05852568. Now the question is: "How confident can I be about these estimates and interpretations?" If we consider the standard error of β_0, we see that it is actually reasonably low, as is the standard error of β_1. Consequently, the 95% confidence interval for β_0 has length 0.428162, meaning that with 95% probability, using the current regression, Catholics' average answer would be between 3.447345 and 3.875507 if Notre Dame's win percentage is zero. Also, the confidence interval for β_1 has length 0.6268003, meaning that with 95% probability a 0.100 increase in Notre Dame's win percentage will increase Catholics' average answer to the question somewhere between 0.02718566 and 0.08986569. The confidence interval indicates that β_1 is statistically significant, meaning that we would reject the null hypothesis H_0: $\beta_1 = 0$. The final decision would seem to be that Notre Dame football has a small but noticeable influence on the nation's Catholics. But one must consider how much of the variation in the dependent variable is being explained by the independent variables. In this case, R2 = 0.0025, meaning that the explained sum of squares (SSE) is 0.0025 as large as the total sum of squares (SST). So, while this regression produced a statistically significant positive estimate for β_1, we are only capturing 0.25% of the variation in the dependent variable attend. This is intuitively feasible; it is easily understood that a person's religious involvement is reliant on many more variables than just Notre Dame football's win percentage.

One might think other possible variables determining religious involvement are a person's age or their family structure. Using the variables associated with these things, I ran a new regression. With the inclusion of the new variables, the estimate of the parameter associated with ndwin and the constant parameter β_0 have changed. In this case, including dummy variables associated with one's marital status means that our interpretation of the constant parameter β_0 has also changed. Here, the dummy variable married has been omitted, so β_0 corresponds to the average answer of married Catholics. Here, the average answer of married Catholics is 3.190043. However, we see that the standard error is large, cre-

age = 35 sqrtage = 5.916 effect on attend = (0.0386796*35) + (-0.1768877*5.916) = 0.3073

age = 36 sqrtage = 6 effect on attend = (0.0386796*36) + (-0.1768877*6) = 0.3311

ating a confidence interval ranging from approximately 1 to more than 5. Using the current model, it is not clear if the estimate of the constant parameter is accurate. The parameters associated with the other marital dummies are all negative, indicating that married Catholics attend Mass more often than those with any other marital status. Also, examining the confidence intervals, all but widow is statistically significant. The hypothesis that the coefficient on widow equals zero could not be rejected. However, similar hypotheses about the other marital dummies could be rejected. Because a person's religious involvement is unlikely to be related to that person's age in a strictly linear manner, the variable sqrtage was included in the regression to allow an estimate of the effect of age on attend to be non-linear. The interpretation of the coefficients of age and sqrtage are more complicated since sqrtage is a function of age. The interpretation is more easily understood with an example: take age first to be, say, 35; then change age to be 36. The coefficients on age and sqrtage determine the effect of that change:

Thus we see that a person 35 years old attends Mass slightly less often than a person 36 years old. However, the confidence intervals both indicate that H_o: $\beta_{age} = 0$ could not be rejected. Therefore, it is not clear if the estimate of the coefficient on age is accurate using the current model. Next, the coefficients on sibs and childs are both positive, indicating that people with children and siblings attend Mass more often than those who do not. Individually, we see that increasing the number of siblings a person has by one will, on average, increase that person's answer by 0.0284537, and adding one child increases the answer by 0.038628. While the coefficient on sibs is statistically significant according to the confidence interval, the coefficient on childs is not. So, we are confident that having siblings has a positive effect on attend, but we are not sure whether having children has a positive, negative, or no effect on attend. Last, we see that the coefficient on ndwin is very close to the estimate attained in the first regression. Also, the standard error is almost identical to the previous estimate. This means that we expect the same effect of ndwin on attend as described before, even when marital status and family structure are accounted for. An examination of the R^2 shows that while it is still rather small, 0.0713, it has increased from the first regression by a factor of more than 28. The significant increase means that this new regression explains approximately 28 times more of the variation in the dependent variable. Therefore, marital status and family structure are important aspects of people's lives in determining their religious involvement.

Continuing the search for aspects of a person's life that affect religious involvement may lead to a consideration of race. Thus another regression was run using variables associated with race. In this case, since the omitted dummies are white and hhwhite, β_o is the average answer of white Catholics living in a predominantly white household. The estimate indicates that the average answer for this group is 3.671705, and the confidence interval is small, meaning that the true value of β_o is very likely to be between 3.453744 and 3.889667. To obtain the average answer of the other groups, the coefficients are added together and to the constant. So those of race other than white or black living in an Asian household gave an average answer of 5.145988. This group gave the highest average answer, but the confidence intervals indicate that rother is not statistically significant. All other variables are statistically significant, and the group with the lowest average answer is those of race other than white or black living in an American Indian household. Their average answer was 2.424085. The estimate of the parameter associated with ndwin is again very close to the original estimate. Notre Dame football has a positive effect on Catholic church attendance when accounting for a person's race. The R^2 is 0.0135, meaning that the current regression explains approximately 1% of the variation in the dependent variable. This is lower than the previous regression, but still much higher than that of the regression of attend on ndwin alone.

One might also wonder whether a person's gender has an effect on his/her religious involvement. This is of course one of the most defining things about a person, so another regression including a variable for gender is needed. In this regression, male is a dummy for whether a person is a male. The omitted group is of course females, so the constant indicates that Catholic women gave an average answer of 3.926007 to the question "How often do you attend religious services?" The coefficient on male shows that men gave an answer that was 0.5898137 lower than women, meaning that men go to Mass less often than women on average. The variable male is statistically significant, as is ndwin. In fact, the estimate of the coefficient on ndwin is again very close to the original estimate. The R^2 is 0.0158, approximately the same as that of the regression with the variables associated to race.

Another very important aspect of a person's life is their career. Thus, a new regression with variables associated with work status was run. In this regres-

sion the omitted dummy variable is wrkfull, so the constant 3.43524 is the average answer given by those who work full-time. This estimate is reasonably accurate, as the confidence interval has length 0.439318. The coefficients on the variables wrkpart, retired, and house are all positive, meaning that people who fall into these categories attend Mass more often than those working full-time, on average. The confidence intervals indicate that all of these variables are statistically significant. The coefficients on tempout, unemp, student, and wother are all negative, indicating that these people attend Mass less often than those working full-time. However, these variables are all statistically insignificant, so it is unclear whether these estimates are accurate. The estimate of the coefficient on ndwin continues to remain similar to the original estimate. Also, $R^2 = 0.0255$, so this regression explains 2.55% of the variation in the dependent variable.

Similar to work status, education plays a large role in the formation of a person. This is possibly one of the most important variables because a person who spends their formative years in school is likely to be far different from a person who did not receive much formal education. So, I ran a regression with the variables educ and ndwin. In this regression, the constant refers to the average answer given by the hypothetical group with zero years of education, when Notre Dame's win percentage was zero. The confidence interval indicates that the true answer is between 2.088707 and 2.811378 with 95% probability. The coefficient on educ indicates that a person with one year of education answered the question on average 0.093069 higher than a person with zero years of education. This is interesting; a more educated person attends Mass more often than an uneducated person according to this regression. One might think that as a person gains more knowledge about the world around him or her, they find it harder to believe in a higher power. But this simple regression indicates that the true tendency is in the opposite direction. The standard error produced a confidence interval of length 0.0441921, meaning that educ is statistically significant and positive. The coefficient on ndwin is similar to the previous estimate, as is the standard error of that estimate. $R^2 = 0.0150$, meaning that this regression explains 1.50% of the variation in the dependent variable.

Another important aspect of a person's life is how that person views the world. Therefore, I ran another regression including variables associated with political affiliation. In this case, the omitted group is Independents. The constant indicates that their average answer Another important aspect of a person's life is how that person views the world. Therefore, I ran another regression including variables associated with political affiliation. In this case, the omitted group is Independents. The constant indicates that their average answer was 3.082873, with standard error 0.129111. The confidence interval has length 0.506218. So, the true value is within .253109 on either side of the estimate with 95% probability. An examination of the coefficients associated with the other party affiliations reveals that they are all positive, and only pidother is statistically insignificant. This means that, with varying degree, a person with any other party affiliation from Independent attends Mass more often than a person identifying him/herself as Independent. The group with the highest attendance answer was the strong Republicans, with an average answer of 4.35954. The $R^2 = 0.0227$, meaning that party affiliation explains 2.27% of the variation in the variable attend. The coefficient on ndwin is slightly lower than previous estimates, but ndwin is still statistically significant and positive.

As a whole, money means a great deal to people, so a person's income becomes almost a defining characteristic of that person. If a person makes a lot more money than some other person, they are likely to live in completely different neighborhoods. While this seems obvious and trivial, this completely determines one's neighbors, proximity to various other locations, children's neighborhood friends, whether a child is allowed to play outside or walk to a friend's house, etc. Thus, a person's perception of his/her family's income can be a very important aspect of that person's life. Therefore, a new regression measuring the effect of family income on church attendance was run. The variable finrela is a scale of a person's perception of his/her family's income in relation to others. The variable is defined on {1,2,3,4,5}. Here, the constant coefficient indicates that a person theoretically answering "0" to the question about family income would on average give an answer to the question about church attendance of 2.96931.

Question: Compared with American families in general, would you say your family income is far below average, below average, average, above average, or far above average?

Respondent's Answer	Entry in Variable finrela
Far below average	1
Below average	2
Average	3
Above average	4
Far above average	5

The coefficient on finrela is 0.2454812, and the confidence interval indicates that finrela is statistically significant. So, a person answering "1" to the income

Linear regression

Number of obs	= 5429
F(9, 5419)	= 6.82
Prob > F	= 0.0000
R-squared	= 0.0108
Root MSE	= 2.5238

attend	Coef.	Robust Std. Err.	t	P>|t|	[95% Conf.	Interval]
ndwin	.5786032	.1597069	3.62	0.000	.2655136	.8916929
midatl	.0632204	.1395701	0.45	0.651	-.2103931	.3368339
encentr	.2282393	.1429669	1.60	0.110	-.0520333	.508512
wncentr	.7241466	.1778833	4.07	0.000	.3754239	1.072869
southatl	-.1006373	.1552037	-0.65	0.517	-.4048989	.2036243
escentr	-.1031726	.3159907	-0.33	0.744	-.7226414	.5162962
wscentr	.1575873	.1602352	0.98	0.325	-.1565381	.4717127
mtn	-.2110219	.1765954	-1.19	0.232	-.5572198	.1351761
pacific	-.2205674	.1507001	-1.46	0.143	-.5160001	.0748653
_cons	3.608334	.1608104	22.44	0.000	3.293081	3.923587

question would give an answer 0.2454812 higher to the church attendance question than the hypothetical person answering "0" to the income question. The coefficient on ndwin is 0.5439477, within 0.05 of the original estimate, and the standard error indicates that ndwin is statistically significant. The R2 = 0.0090, which is lower than most of the previous regressions. This is understandable because here there are only two independent variables, and finrela is not a specific monetary value, but rather a rough scale.

A person's income can determine in which neighborhood that person lives. A question rising from that thought is: "How does regional residence affect Catholic church attendance?" One might wonder whether living in New England has a different effect on church attendance than living in the mountain region. Another regression was run using variables associated with regional residence. Here, the omitted group is those living in New England, so the constant of 3.608334 means that those living in New England gave that as an average answer to the question about church attendance.

The coefficient on ndwin is within 0.01 of the original estimate, and the standard error is within 0.0002 of the original estimate of standard error. Examining the variables associated with the other regions of the country shows that the coefficients on midatl, encentr, wncentr, and wscentr are positive, meaning that people in these regions attend Mass more often than the people in New England, on average. On the other hand, the coefficients on the variables southatl, escentr, mtn, and pacific are negative, meaning that people in these regions attend Mass less often than those in New England. Interestingly however, only the variable wncentr is statistically significant of all the regional dummy variables. So, it can be said that people in the West North Central region attend Mass more often than those in New England, but not much else can be said about the region in which a person lives in terms of the effect on church attendance. The coefficient on ndwin remains similar to the previous estimate, and $R^2 = 0.0108$. This means that regional residence explains only 1% of the variation in Catholic attendance at Mass.

In all previous regressions, the focus has been on nonreligious aspects of a person's life. Only those people who identified themselves as Roman Catholic in the survey have been considered. However, a person's religious past likely plays a large role in their current religious involvement. In the GSS, people were asked what their religious affiliation was when they were 16 years old. So, I ran another regression including variables associated with past religious affiliation. The omitted group is those who were Roman Catholic at age 16. Their average answer was 3.63396 with confidence interval of length 0.4319. This regression yields interesting results: only those identifying themselves as Jewish or with no religious affiliation at age 16 attend Mass less often than those who were Roman Catholic at age 16. The standard error of the coefficient on jew is more than five times greater than the estimate itself. Therefore, almost nothing decisive can accurately be said about the variable jew. The standard error of the coefficient on none is also high, but not high enough to render none statistically insignificant. The coefficients on the other variables (prot, r16other, budd, muslim, orthod, and christ) are all positive. This means that the people in those groups actually attend Mass more often than those people who were Catholic at age 16. Of these variables, only orthod is statistically insignificant, so we can be reasonably certain that the people in the groups prot, r16other, budd, muslim, and christ actually do attend Mass more often than those in cath, on average. The estimates of the coefficients on budd, muslim, and christ are very

Linear regression

Number of obs	= 5429
F(8, 5419)	= .
Prob > F	= .
R-squared	= 0.0067
Root MSE	= 2.529

attend	Coef.	Robust Std. Err.	t	P>|t|	[95% Conf.	Interval]
ndwin	.5935587	.159859	3.71	0.000	.2801709	.9069466
prot	.3624895	.1332363	2.72	0.007	.1012927	.6236863
jew	-.1645086	.8600041	-0.19	0.848	-1.850462	1.521445
none	-.687646	.2839947	-2.42	0.015	-1.24439	-.1309022
r16other	1.084032	.4700679	2.31	0.021	.1625099	2.005554
budd	2.362888	.4155548	5.69	0.000	1.548233	3.177542
muslim	2.046706	.0403544	50.72	0.000	1.967595	2.125817
orthod	1.801157	.9874679	1.82	0.068	-.1346764	3.736991
christ	2.132178	.7701967	2.77	0.006	.6222832	3.642073
_cons	3.63396	.110156	32.99	0.000	3.41801	3.84991

high (above 2), and the confidence interval of christ includes values as low as .6222832 and as high as 3.642073. This variation is huge; it means that those identifying themselves as simply being Christian at age 16 could have answered 4.2562432 on average, or they could have answered 7.276033, on average! The coefficient on ndwin is again similar to the original estimate, as is its standard error. However, the R^2 = 0.0067, meaning that one's religious past explains a remarkably small amount of the variation in current Mass attendance.

The previous regressions have accounted for many facets of a person's life, and hopefully a large part of their decision as to how often to attend Mass is included in the variables. A more complete understanding of why people attend Mass, or not, will lead to better knowledge of the effect of Notre Dame's football team on Catholic church attendance. A regression including all the variables discussed above must be run to determine this effect. The regression yields a constant value of -0.1032075, with standard error 0.2917655. The confidence interval is [-0.6751861, 0.4687711]. Interpreting the constant value in this case is very difficult; because of the many dummy variables and many omitted groups, the constant refers to a female, living in New England, who was Catholic at age 16, is married, etc. Even understanding what the constant value technically means does not shed much light on how to really interpret this value. Similarly, the coefficients on the other variables are more difficult to understand than before. However, the task of this study is to interpret only one coefficient. The estimate of coefficient on the variable ndwin is 0.5401791 with robust standard error 0.1514687 and 95% confidence interval [0.2432392, 0.837119], and the R^2 for this regression is 0.1402. The Stata results for this regression are attached to the online version of the paper.

Conclusion

Does the success of the Notre Dame football team have an effect on Catholic attendance at Mass? The lives of human beings are infinitely complex. A person's religious beliefs and tendencies are among the least explainable aspects of his/her life. The faithful are comprised of all types of people, from different parts of the world, with varying social status and family structures. The R2 of the regression detailed on the next page is 0.1402; 14% of the variation in church attendance is explained by the 47 variables included in the regression. The coefficient β_{ndwin} is 0.5401791; an increase in Notre Dame's win percentage by 0.100 will, on average, increase respondents' answers to the question "How often do you attend religious services?" by 0.05401791. This is a small number, but if one imagines an increase in Notre Dame's win percentage by 0.500 from one year to the next, then the average response to the question above is expected to increase by 0.27008955. This may still be a small effect, but the effect does exist. The standard error of β_{ndwin} is 0.1514687, meaning that the 95% confidence interval does not include zero. Therefore, the null hypothesis Ho: $\beta_{ndwin} = 0$ can be rejected.

So, there exists a small but statistically significant positive relationship between the win percentage of the Notre Dame football team and American Catholic church attendance as measured by the General Social Survey.

Source: The data used to conduct this study was obtained from the publicly available GSS-STATA download located at: http://www.norc.org/GSS+Website/Download/STATA+v8.0+Format/

This paper has been written as the final project for Prof. Dan Hungerman's Fall 2009 Econometrics course. I would like to thank Prof. Hungerman for his exemplary teaching skills and for setting this enjoyable and rewarding assignment.

Prime Numbers And Information Security

Bethany Herwaldt

University of Notre Dame, Department of Mathematics

Abstract

Have you ever wondered how your credit card information is communicated securely on the Internet? It turns out that prime numbers are key. A popular method of encryption for e-commerce is the RSA algorithm. This algorithm relies on the fact that it is easy to find a large prime number but difficult to factor a large composite number. We will detail several methods of finding large prime numbers called primality tests. Most of these tests only come to the conclusion that there is a high probability that a certain number is prime. Until 2002, this was the best mathematicians could do without using a test that was so computationally complex that it was useless. However, in 2002, a new computationally feasible test called AKS was discovered that will tell with certainty whether or not a number is prime. We will end with an explanation of how primality tests are used in the RSA cryptosystem to keep information secure.

1. Introduction

Prime numbers are the building blocks of all integers; every integer is either prime or a product of prime numbers. Prime numbers have fascinated humans since at least 1600 BC, yet mathematicians continue to make discoveries about their fundamental properties. Around 300 BC, Euclid proved that there are infinitely many primes, but we still do not have a formula to list them. There was no known application of prime numbers until the 1970s when people realized that prime numbers could be used as the basis of a secure cryptosystem. This discovery renewed the drive to find an efficient primality test, a test that determines whether or not a number is prime.

2. Preliminaries

Before we can learn about primality tests and RSA encryption, we need to define some notation and learn some basic number theory, the study of integers. We will use the notation "$a \in S$" to mean that a is an element in the set S. We will use the notation "$n \in \mathbb{Z}$" to mean that n belongs to the set of integers. The proofs of some of the theorems in this section will be omitted, but they can be found in an introductory number theory book such as Yan's *Number Theory for Computing*.

Now we need to learn about modular arithmetic, a special system of arithmetic specifically for integers. This may seem strange at first, but understanding it will be crucial to understanding the rest of the article. Also, I will teach you why you can truthfully tell your friends that two plus two is one, as long as you mutter "modulo 3."

Do you remember learning division in elementary school? Sometimes, we would write an answer to a long division problem as "5 R 2," meaning that after dividing, we had a remainder of 2. We can split the integers into n classes based on the remainder after dividing by n. One example would be division by 3. You can group the integers by their remainder after dividing by 3:

Class 0 : $0, 3, 6, 9, 12, 15, \ldots$
Class 1 : $1, 4, 7, 10, 13, 16, \ldots$
Class 2 : $2, 5, 8, 11, 14, 17, \ldots$

We say that an integer a is equivalent to b modulo n if the remainder of a when dividing by n is b. We denote this as $a \equiv b \mod n$. To return to our example, $14 \equiv 2 \equiv 5 \mod 3$ because $14 = 4 \cdot 3 + 2$ and $5 = 1 \cdot 3 + 2$. Note that $2 + 2 = 4 \equiv 1 \mod 3$ because $4 = 1 \cdot 3 + 1$. Thus, two plus two is one modulo 3, as promised. Tell your friends.

Definition 1. $a \equiv b \mod n$ if and only if $a = kn + b$ for some $k \in \mathbb{Z}$.

From this definition, we can immediately notice several properties of modular arithmetic which we will use repeatedly. We can add to, subtract from, or multiply both sides. We will see in Theorem 8 that we cannot always divide both sides. Also, addition preserves equivalences.

Theorem 1.

1. *If* $a + c \equiv b + c \mod n$, *then* $a \equiv b \mod n$.
2. *If* $a \equiv b \mod n$, *then* $ac \equiv bc \mod n$.
3. *If* $a \equiv c \mod n$ *and* $b \equiv d \mod n$, *then* $a + b \equiv c + d \mod n$.

[1]This article is based on part of the author's Senior Thesis, being written under the supervision of Prof. D. Galvin, Department of Mathematics.

Proof.

1. Suppose $a + c \equiv b + c \mod n$. Then $(a + c) = kn + (b + c)$ and $a = kn + b$. Thus, $a \equiv b \mod n$.
2. Suppose $a \equiv b \mod n$. Then $a = kn + b$. Then $ac = (ck)n + bc$. Thus, $ac \equiv bc \mod n$.
3. Suppose $a \equiv c \mod n$ and $b \equiv d \mod n$. Then $a = k_1 n + c$ and $b = k_2 n + d$ for some integers k_1 and k_2. Then $a + b = k_1 n + c + k_2 n + d = (k_1 + k_2)n + (c + d)$. This means that $a + b \equiv c + d \mod n$.

□

An important concept in number theory is whether or not one integer divides another integer evenly. We want to know if that long division is going to end with a nice "R 0."

Definition 2. Let $a, n \in \mathbb{Z}$ with $n \neq 0$. We say that n *divides* a if $a = kn$ for some $k \in \mathbb{Z}$, or if $a \equiv 0 \mod n$. This is denoted $n \mid a$.

If n does not divide a, we denote $n \nmid a$. If $n \mid a$, then n is called a *divisor* of a. We now have a new way to define congruence modulo n.

Definition 3. $a \equiv b \mod n$ if and only if $n \mid (a - b)$.

Why is this true? Start with the left. If $a \equiv b \mod n$, then we can subtract b from both sides and see that $a - b \equiv 0 \mod n$. By the definition of division given above, then $n \mid (a - b)$. Now start with the right. Suppose $n \mid (a - b)$. Then we know that $a - b \equiv 0 \mod n$. We add b to both sides and find that $a \equiv b \mod n$.

Notice that we now have three equivalent statements:

1. $a \equiv b \mod n$
2. $a = kn + b$ for some integer k
3. $n \mid (a - b)$

Three definitions may seem excessive, but we will switch between them frequently throughout this article. Let's practice. Suppose we discover that $a^{687} \equiv 35b + 14 \mod 7$. Then we can also say that $a^{687} = 7k + 35b + 14$ for some integer k and $7 \mid (a^{687} - 35b - 14)$.

Two properties of division that we will use again are:

Theorem 2.

1. *Suppose that $a \mid b$ and $a \mid b + c$. Then $a \mid c$.*
2. *Suppose that $a \mid b$ and $b \mid c$. Then $a \mid c$.*

Proof.

1. Let $a \mid b$ and $a \mid b + c$. Then $b \equiv b + c \equiv 0 \mod a$. We can subtract b from both sides to see that $0 \equiv c \mod a$. Thus, $a \mid c$.
2. Let $a \mid b$ and $b \mid c$. Then $ak_1 = b$ and $bk_2 = c$ for some integers k_1 and k_2. Then $ak_1k_2 = c$, so $a \mid c$.

□

You may recall the greatest common divisor from grade school, but next we will state a formal definition.

Definition 4. Let a and b be positive integers. Suppose $d \mid a$ and $d \mid b$. Then d is a divisor of both a and b. Suppose also that for any integer c such that $c \mid a$ and $c \mid b$, it is also true that $c \mid d$. Then d is the *greatest common divisor* of a and b, denoted $\gcd(a, b)$.

For example, $1960 = 2^3 \cdot 5 \cdot 7^2$ and $15092 = 2^2 \cdot 7^3 \cdot 11$, so $\gcd(1960, 15092) = 2^2 \cdot 7^2 = 196$.

Now we can state another property of division that will be useful later.

Theorem 3. *Suppose that $a \mid c$ and $b \mid c$. Then $\gcd(a, b) = 1$ implies $ab \mid c$.*

"Euclid's algorithm," written around 300 BC, is a quick way to calculate the greatest common divisor without knowing the prime factorization of the two numbers. We will refer back to this algorithm later. First, we will state the theorem on which Euclid's algorithm is based.

Theorem 4. *Let $a, b, q, r \in \mathbb{Z}$, where b is positive and $0 \leq r < b$ such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

What does this theorem mean? Suppose we want to find the greatest common divisor of two large numbers a and b, with $a > b$. This might be difficult because they are so big. Instead, we can divide a by b to find a suitable q_0 and r_0 such that $a = bq_0 + r_0$ where r_0 is smaller than b. Then we

can instead find the greatest common divisor of b and r_0. It may be that b and r_0 are still large, but we could do this process repeatedly. Next we find q_1 and r_1 such that $b = r_0q_1 + r_1$ where $0 \leq r_1 < r_0$. When do we stop this process? We know that if we keep forcing the r_i's to decrease, yet stay greater than or equal to 0, the process has to end. In particular, it will end when we reach a remainder of 0. What have we done?

$$\begin{aligned} a &= bq_0 + r_0 & 0 \leq r_0 < b \\ b &= r_0q_1 + r_1 & 0 \leq r_1 < r_0 \\ r_0 &= r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ &\dots & \dots \\ r_{n-2} &= r_{n-1}q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0 & r_{n+1} = 0 \end{aligned}$$

By repeatedly using Theorem 4, this means that $\gcd(a,b) = \gcd(b,r_0) = \dots = \gcd(r_{n-1},r_n)$. Since $r_{n+1} = 0$, we know that $r_n \mid r_{n-1}$ and thus r_n is the $\gcd(r_{n-1},r_n)$. We can then conclude that $\gcd(a,b) = r_n$. The significance of this algorithm is that it is fast and does not require knowledge of the prime factorization of a and b. Specifically, if b has d decimal digits, it can be shown that the algorithm will take at most $5d$ steps (Koblitz 14). This means that if you wanted to find the greatest common divisor of two 200 digit numbers, it would take at most 1,000 steps using this algorithm, or a fraction of a second on a fast computer. In comparison, if you tried to find the greatest common divisor by first finding the prime factorization of each number, even if you used the fastest available computers and the best known factorization algorithms, it would probably take years. Thus, Euclid's algorithm, discovered thousands of years ago, is an amazing acceleration of this process.

Let's write this algorithm formally.

Theorem 5. Euclid's Algorithm *Let a and b be positive integers with $a > b$. If $b \mid a$, then $\gcd(a,b) = b$. If $b \nmid a$, then divide b into a, finding a remainder r_0. Next, divide r_0 into b, finding a remainder r_1. Continue this process until the remainder r_{n+1} is 0. Then $r_n = \gcd(a,b)$.*

As an example, remember that we stated above that $\gcd(1960, 15092) = 196$. Let's find the same answer using Euclid's Algorithm.

$$\begin{aligned} 15092 &= 1960 \cdot 7 + 1372 & 0 \leq 1372 < 1960 \\ 1960 &= 1372 \cdot 1 + 588 & 0 \leq 588 < 1372 \\ 1372 &= 588 \cdot 2 + 196 & 0 \leq 196 < 588 \\ 588 &= 196 \cdot 3 + 0 & 0 = 0 \end{aligned}$$

Now we can state one consequence of Euclid's algorithm that is frequently used.

Theorem 6. *For any positive integers a and b, there exist integers x and y such that $ax + by = \gcd(a,b)$.*

This can be proven by manipulating the series of equations produced in the process of Euclid's algorithm.

An immediate result of this theorem that we will be using is that if $\gcd(b,n) = 1$, then b has an inverse b' modulo n. In other words, $bb' \equiv 1 \mod n$. This is because we are able to find integers x and b' such that $an + bb' = 1$. Note that this is certainly not true in normal arithmetic. The inverse of an integer b in normal arithmetic is $1/b$, which is not another integer unless $b = 1$. However, for example, the inverse of 3 modulo 5 is 2 because $3 \cdot 2 = 6 \equiv 1 \mod 5$.

Theorem 7. *Let b and n be positive integers such that $\gcd(b,n) = 1$. Then there exists another positive integer b' such that $bb' \equiv 1 \mod n$. In other words, b has an inverse modulo n.*

Proof. By Theorem 6, there exist integers x and y such that $nx+by = \gcd(b,n) = 1$. Then $by = -nx+1$ and thus $by \equiv 1 \mod n$. If y is not positive, we pick a positive b' such $b' \equiv y \mod n$. □

Modular arithmetic does not operate in the same fashion as regular arithmetic. One difference is that you cannot always divide both sides by a number. Consider the following theorem.

Theorem 8. *If $a \neq 0$, $ax \equiv ay \mod n$ if and only if $x \equiv y \mod \left(\frac{n}{\gcd(a,n)}\right)$.*

In particular, this theorem means that you can divide both sides of an equivalence modulo n by a if and only if a and n have no common factors. Recall from Theorem 1 that we can always multiply both sides.

Since this article is all about prime numbers, we should make sure we know the technical definition.

Definition 5. A positive integer $n > 1$ is called *prime* if its only divisors are 1 and itself. Otherwise, it is called *composite*.

Recall that two numbers a and b are called coprime if $\gcd(a, b) = 1$. In other words, they are coprime if they have no common divisors.

An important basic fact about integers is the Fundamental Theorem of Arithmetic:

Theorem 9. Fundamental Theorem of Arithmetic *Every positive integer n greater than* 1 *can be written uniquely as a product of distinct primes:*

$$n = \prod_{i=1}^{k} {p_i}^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where each p_i is a distinct prime and each α_i is a natural number. This product is called the standard prime factorization of n.

For example, $363528 = 2^3 \cdot 3^5 \cdot 11 \cdot 17$.

This theorem is proven using Euclid's observation that if a prime number p divides a product ab, then p divides a or b. For example, $3 \mid 6 \cdot 10$, so $3 \mid 6$ or $3 \mid 10$. This is not necessarily true for a composite number. $6 \mid 9 \cdot 4$ but $6 \nmid 9$ and $6 \nmid 4$. We will also use this observation later in this article.

In order to understand several of the following concepts in this article, including how the AKS algorithm works, we need to know about "order."

Definition 6. Let a and m be positive integers such that $\gcd(a, m) = 1$. Then the *order* of a modulo m is the smallest integer k such that $a^k \equiv 1 \mod m$.

For example, the order of 3 modulo 11 is 5.

$$3^1 = 3 \equiv 3 \mod 11$$
$$3^2 = 9 \equiv 9 \mod 11$$
$$3^3 = 27 \equiv 5 \mod 11$$
$$3^4 = 81 \equiv 4 \mod 11$$
$$3^5 = 243 \equiv 1 \mod 11$$

One reason to consider the order of a number is the following useful theorem.

Theorem 10. *Let k be the order of a modulo m. If $a^n \equiv 1 \mod m$ then $k \mid n$.*

We will also be using primitive roots, Euler's totient function and one of Euler's many theorems, the Euler Totient Theorem.

Theorem 11. *Let p be a prime number. Then there exists an integer a, called the primitive root, such that $p - 1$ is the order of a modulo p.*

Definition 7. *Euler's totient function, ϕ,* is defined as $\phi(n)$ equals the number of integers $\leq n$ coprime to n.

For example, consider the number 10. It has common factors with 2, 4, 5, 6, and 8. 10 is coprime to 1, 3, 7, and 9. Thus, $\phi(10) = 4$. Fortunately, this function can be computed without checking every number less than n.

Theorem 12. *Let n be an integer. Use the fundamental theorem of arithmetic to write n's standard prime factorization: $n = \prod_{i=1}^{k} {p_i}^{\alpha_i}$. Then*

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Returning to the previous example, $10 = 2 \cdot 5$. Then

$$\phi(10) = 10\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{5}\right) = 10\left(\tfrac{2-1}{2}\right)\left(\tfrac{5-1}{5}\right)$$
$$= 10\left(\tfrac{1}{2}\right)\left(\tfrac{4}{5}\right) = 4\,.$$

Note that if p and q are primes, then $\phi(p) = p - 1$ and $\phi(pq) = (p - 1)(q - 1)$.

Now we are ready to state Euler's Totient Theorem. It is a generalization of Fermat's Little Theorem, which we will state and prove in section 3.2 as Theorem 15.

Theorem 13. Euler's Totient Theorem *If a and n are positive integers such that* $\gcd(a, n) = 1$, *then $a^{\phi(n)} \equiv 1 \mod n$.*

Now that we have learned about modular arithmetic, dividing, greatest common divisors, prime numbers, and order, we are ready for the meat of the article, primality tests.

3. Primality Tests

3.1. Probable Primes and Pseduoprimes

The RSA cryptosystem works under the assumption that it is easy to find two large prime numbers but difficult to factor a large composite number. How do we find a prime number?

First, we decide how large of a number we need, say 100 digits. Next, we randomly select numbers that have that many digits and test to see if they are prime. We do this repeatedly until we find a prime number.

Will we ever find a prime number with 100 digits? How many 100-digit prime numbers are there? Mathematicians have long been studying how the prime numbers are distributed. Since the 1700s, mathematicians have been postulating and proving various approximations for $\pi(x)$, the number of prime numbers less than or equal to x. The most famous approximation is that $\pi(x) \sim \frac{x}{\ln x}$. In other words,

Theorem 14. Prime Number Theorem

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1\,.$$

This means that between 10^{99} and 10^{100}, there are approximately

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln(10^{100})} - \frac{10^{99}}{\ln(10^{99})} \approx 3.90\times 10^{97}$$

prime numbers, or that about .434% of 100 digit integers are prime. So, about 1 in 256 100-digit numbers are prime. If you had a quick primality test, you would expect to on average have to run it about 256 times before finding a prime.

How do we decide whether or not a number n is prime? Well, we could look back to the definition of a prime number. It must not have any divisors other than 1 and itself. So, one method would be to divide n by every number less than n and see if any numbers divide evenly. Actually, if we had a list of smaller primes, we could just divide n by every prime number $\leq \sqrt{n}$. However, we are talking about 100 digit numbers. That would take far too long. Fortunately, there are more efficient tests.

We've been making vague references to procedures being "fast enough." In order to appreciate the differences between the algorithms we will present and the significance of the AKS algorithm, we will give an introduction to computational complexity. When people design algorithms, it is important to consider how quickly an algorithm will run, or its "running time." If the algorithm is too computationally intensive, it will not actually be practical. What good is an algorithm which, even with all of the computing power in the world, would take thousands of years to run?

We classify algorithms based on which function approximately represents how many operations will be used. The following table gives examples.

n	$\log_2 n$	n^2	2^n
5	2	25	32
10	3	100	1024
10^2	6	10^4	1.27×10^{30}
10^5	16	10^{10}	9.99×10^{30102}

It is clear that, for example, that the growth of 2^n is much faster than the growth of $\log_2 n$. An algorithm is considered practical if it falls into the category of n^k for some constant k. In more technical terms, we wish for an algorithm that is $O(n^k)$, also known as *polynomial time*. What does this notation mean?

Definition 8. Let $f(n)$ be a function and k be a constant. Then $f(n) = O(n^k)$ as $n \to \infty$ if and only if $\left|f(n)\right| \leq Mn^k$ for $n > n_0$ for some positive real number M and some real number n_0.

This notation may still seem odd to you, but it allows us to define our "category." Suppose an algorithm takes $f(n) = 50n^3 + 23000n^2$ steps. Then $\left|f(n)\right| = 50n^3 + 23000n^2 \leq 51n^3$ for all $n \geq 23000$. Thus, $f(n) = O(n^3)$. We only need to consider the highest degree in $f(n)$ because as n approaches infinity, the smaller terms will become insignificant. If an algorithm requires several steps, we add the running times of each algorithm. Again, the fastest growing step is the only one that matters. If the number of steps is dependent on the size of n then adding these running times is essentially multiplying by another function of n. For example, if each step takes n operations and there are n steps, then the running time is $O(n^2)$.

In the context of this paper, we judge the complexity of an algorithm based on how many bit operations it will take to run on a number n with d binary digits. When a number is written in binary, each digit, a 1 or a 0, is called a bit. Adding two numbers that each have d binary digits requires d bit operations. The number of binary digits

in a number n is $\lfloor \log_2 n \rfloor + 1$, where $\lfloor a \rfloor$ means a rounded down to the next integer. For example, $\log_2 8 = 3$ and $\log_2 50 \approx 5.64$ so we know that 8 has 4 digits and 50 has 6 digits in binary. This is confirmed by noting that 8 is written as 1000 and 50 is written as 110010 in binary. Since in computational complexity, we are concerned about very large numbers, we can simplify our notation and just write $\lfloor \log_2 n \rfloor$ for the number of binary digits (Koblitz 3).

We of course expect there to be more operations on a number with more digits. We know that in adding two binary numbers with the same number of binary digits, the number of bit operations is equal to the number of binary digits, $\lfloor \log_2 n \rfloor$. Multiplying two numbers using the same procedure that we are taught in school takes about $O((\log_2 n)^2)$ bit operations. There exist more efficient algorithms, but for the purpose of this paper we will use this time estimate. Division of an integer with $2\log_2 n$ digits by another integer with $\log_2 n$ digits also takes $O((\log_2 n)^2)$ operations.

Since we are concerned with bit operations, we actually wish for the category of $O((\log_2 n)^k)$. Let's put this in practical terms. Suppose that we have one year to decide if a number is prime on a Jaguar supercomputer. Assuming that this computer maintained its peak performance of 1.75×10^{15} instructions per second, it could complete about 5.5×10^{22} instructions in a year. If we decide to use trial division and divide n by every prime up to and including $\sqrt{n}$, then we have on the order of $O(\pi(n^{1/2})(\log_2 n)^2) = O(\frac{n^{1/2}}{(\ln n)^{1/2}}(\log_2 n)^2) = O(n^{1/2}(\log_2 n)^{3/2})$ bit operations. The Jaguar would be able to determine whether or not a 39 digit number was prime, but probably nothing larger. The Fermat Test, the first test that we are going to describe, is $O((\log_2 n)^3)$ bit operations, so the Jaguar would be able to handle a $10,000,000$ digit prime in one year. As you can clearly see, an algorithm that takes polynomial time is a vast improvement over trial division.

There are two types of primality tests, probabilistic and deterministic. Deterministic tests tell that a number is definitely a prime. Probabilistic tests say that a number is probably a prime. Most probabilistic tests have the same form. We know that all prime numbers have Property C. Suppose a number n has Property C. Is it a prime number? Ideally, we choose a property that few composite numbers have. If n has Property C, we call it a "C-probable prime." If we know that the number is actually composite, we call it a "C-pseudoprime." If the probability that a certain "C-probable prime" is really a prime is sufficiently high, it can be used in such applications as RSA and is called an "industrial-grade prime" (Crandall 119-120). An example of a poor choice for Property C would be "either 2 or odd." This is indeed a property of all primes, but it is also a property of many composite numbers. We will now consider several tests relying on more appropriate properties.

3.2. Fermat Primality Test

One probabilistic primality test relies on Fermat's Little Theorem.

Theorem 15. Fermat's Little Theorem *If b is a positive integer, p is a prime, and* $\gcd(b,p) = 1$, *then*

$$b^{p-1} \equiv 1 \mod p\,.$$

Proof. Let b be any positive integer, p be a prime, and $\gcd(b,p) = 1$. We wish to show that $b^{p-1} \equiv 1 \mod p$. Consider the values $b \bmod p, 2b \bmod p, 3b \bmod p, \ldots, (p-1)b \bmod p$. Since $\gcd(b,p) = 1$, we know that these $p-1$ values are all distinct, and none are equivalent to 0. Suppose that two of these values were *not* distinct. Then $k_1 b \equiv k_2 b \bmod p$. By Theorem 7, b has an inverse modulo p. We will call it b'. We can multiply both sides of the last equation and find that $k_1 bb' \equiv k_2 bb' \bmod p$, or $k_1 \equiv k_2 \bmod p$. This is impossible, since both k_1 and k_2 are less than p and p is prime. Thus, each of the $p-1$ values really are distinct. Recall that considering numbers modulo p splits the integers into p classes, those equivalent to $0, 1, 2, \ldots, p-1$. Since we have $p-1$ numbers that all have distinct values when considered modulo p and none are equivalent to 0,

$$\begin{aligned} b \cdot 2b \cdot 3b \cdots (p-1)b &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p \\ (p-1)!b^{p-1} &\equiv (p-1)! \mod p \end{aligned}$$

We know that $\gcd(p,(p-1)!) = 1$ since p is prime, so we can divide both sides by $(p-1)!$. We find $b^{p-1} \equiv 1 \mod p$ (Yan 124). □

Note that by Theorem 1, this theorem equivalently states that $b^p \equiv b \mod p$. When Fermat's Little Theorem is written this way, we no longer require that $\gcd(b,p) = 1$. Suppose that $\gcd(b,p) \neq 1$. Then $p \mid b$, so both b^p and b are equivalent to 0 modulo p. Thus, $b^p \equiv b \mod p$ is still true.

Clearly, this theorem gives an example of a property of all prime numbers. Suppose $b^n \equiv b \mod n$. We call n a Fermat probable prime base-b. You may hope that only a small number of these are pseduoprimes. We first prove the unfortunate fact that there are infinitely many pseudoprimes for each base. We then state without proof the good news, that Fermat pseduoprimes are rare compared to primes.

Theorem 16. *For each integer $a \geq 2$, there exist infinitely many Fermat pseudoprimes base a.*

Proof. We will show that for each odd prime p that does not divide $a^2 - 1$, $n = (a^{2p} - 1)/(a^2 - 1)$ is a pseudoprime base a. This n is certainly an integer, as we know $(a^2)^p - 1 = (a^2 - 1)((a^2)^{p-1} + (a^2)^{p-2} + (a^2)^{p-3} + \ldots + a^2 + 1)$. Since $a^2 - 1$ can only have finitely many prime factors, there must be infinitely many primes that do not divide it. Thus, if the first sentence is true, we have infinitely many base-a pseudoprimes.
First, we note that n is indeed composite. In particular, it can be factored as

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}.$$

Now we wish to show that $a^{n-1} \equiv 1 \mod n$. Note that $n - 1 = (a^{2p} - a^2)/(a^2 - 1)$. Since p is prime, we know $a^p \equiv a \mod p$ by Fermat's Little Theorem. By squaring both sides, we find that $a^{2p} \equiv a^2 \mod p$. This means that $p \mid a^{2p} - a^2 = (a^2 - 1)(n - 1)$. However, we assumed that $p \nmid a^2 - 1$. Thus, $p \mid n - 1$.

Now consider the identity

$$n - 1 = a^{2p-2} + a^{2p-4} + \cdots + a^2,$$

which we can see by the definition of n and the above factorization of $a^{2p} - 1$. We see that $n - 1$ is the sum of an even number of terms, and the terms must either all be odd or all be even. This means that $n - 1$ is even. Since both 2 and p divide $n - 1$ and p is an odd prime, we now know that $2p \mid n - 1$. This means that $n - 1$ can be written $n - 1 = k(2p)$ for some integer k. Thus, $a^{n-1} - 1 = a^{k(2p)} - 1^{2p} = (a^{2p} - 1)((a^{2p})^{k-1} + (a^{2p})^{k-2} + (a^{2p})^{k-3} + \ldots + (a^{2p}) + 1)$. Then $a^{2p} - 1 \mid a^{n-1} - 1$. By the definition of n, we know $n \mid a^{2p} - 1$. Thus, $n \mid a^{n-1} - 1$, which means $a^{n-1} \equiv 1 \mod n$ and $a^n \equiv a \mod n$ (Crandall 121). □

Theorem 17. *Fermat pseudoprimes are rare compared with primes. Specifically, fix an integer $a \geq 2$. Denote the number of Fermat pseudoprimes base a that are less than or equal to x as $p_a(x)$. Then*

$$\lim_{x \to \infty} \frac{p_a(x)}{\pi(x)} = 0.$$

In other words, the number of prime numbers less than x grows much more rapidly than the number of Fermat pseudoprimes base a. If you are interested in the proof of this theorem, see Paul Erdős' paper "On Almost Primes" from 1950.

We can repeat this test for various bases and thus increase the probability that a number is really prime. If you test a number for enough bases, will you eventually know for sure that the number is prime? Unfortunately, the answer is no. There exist composite numbers that will pass the test for every base.

Definition 9. Let n be a composite number that it is a base-b pseudoprime for every $2 \leq b \leq n$. Then we call n a *Carmichael number*.

We can exactly describe which set of numbers will be Carmichael numbers, although the set of conditions would take a long time to check for any sizable number.

Theorem 18. *An integer n is a Carmichael number if and only if n is positive, composite, square-free, and for each prime divisor p of n, $p - 1 \mid n - 1$.*

To clarify, a number n is called square-free if there are no squared integers that divide n. This means, for example, that $4, 9, 16$, and 25 do not divide n.

Proof. Note that this theorem contains the phrase "if and only if." This proof will contain two major parts. First, we will prove that a number is a Carmichael number *only if* it has those four properties. In other words, every Carmichael number has them. Second, we will prove the *if* part,

that any number with those four properties is a Carmichael number.

Suppose n is a Carmichael number. Then we know n is positive and composite. We wish to show that it is square-free and for each prime divisor p of n, $p-1 \mid n-1$. Suppose that n is actually not square-free. Then there is a prime divisor p of n such that $p^2 \mid n$. Then $n = p^2 k_1$ for some integer k_1 and $p^{n-2}n = p^n k_1$. Since n is a Carmichael number, we know $p^n \equiv p \mod n$. Then $p^n = k_2 n + p$ for some integer k_2. Thus,

$$\begin{aligned} (k_2 n + p)k_1 &= p^{n-2}n \\ k_1 k_2 n + k_1 p &= p^{n-2}n \\ k_1 p &= n(p^{n-2} - k_1 k_2) \end{aligned}$$

Then $n \mid k_1 p$. However, $n = p^2 k_1$ so $p^2 k_1 \mid k_1 p$. This is a contradiction, so our assumption that $p^2 \mid n$ must be false. n must be square-free.

Let p be a prime divisor of n. We wish to show that $p-1 \mid n-1$. Let a be a primitive root modulo p. Then $a^{p-1} \equiv 1 \mod p$. Since n is a Carmichael number, we know that $a^{n-1} \equiv 1 \mod n$, so $n \mid a^{n-1} - 1$. Since $p \mid n$, $p \mid a^{n-1} - 1$ and thus $a^{n-1} \equiv 1 \mod p$. Since the order of a modulo p is $p-1$ and $a^{n-1} \equiv 1 \mod p$, we know $p-1 \mid n-1$. Thus, the proof is finished in one direction.

Now we wish to show the other direction. Assume that an integer n is positive, composite, square-free, and that for each prime divisor p of n, $p-1 \mid n-1$. We want to show that n is a Carmichael number. In other words, we want to show that for any positive integer a, $a^n \equiv a \mod n$. Since we know that n is square-free, if each prime divisor divides $a^n - a$, then surely $n \mid a^n - a$. Thus, it is only necessary to show that for each prime divisor p of n, $a^n \equiv a \mod p$, or equivalently that $p \mid a^n - a$.

Suppose $\gcd(a,p) = 1$. By Fermat's Little Theorem, we know that $a^{p-1} \equiv 1 \mod p$. We know that each $p-1 \mid n-1$, so $(p-1)k = n-1$ for some integer k. Then $a^{n-1} \equiv a^{(p-1)k} \equiv 1^k \equiv 1 \mod p$ as well, and $a^n \equiv a \mod p$. Suppose $\gcd(a,p) \neq 1$. Then $p \mid a$, so clearly $p \mid a^n - a$ and thus $a^n \equiv a \mod p$. Therefore, for any a, $a^n \equiv a \mod p$ and n is a Carmichael number (Crandall 122). □

The smallest Carmichael number is 561. We can use this theorem to verify that it is a Carmichael number. Clearly 561 is positive. It is also composite and square-free because it can be factored as $3 \cdot 11 \cdot 17$. For each prime divisor p of 561, does $p - 1 \mid 560$? Yes, $2 \mid 560$ because $560 = 2 \cdot 280$, $10 \mid 560$ because $560 = 10 \cdot 56$, and $16 \mid 560$ because $560 = 16 \cdot 35$.

It is known that there are infinitely many Carmichael numbers. In 1956, Paul Erdős gave a heuristic argument in his paper "On Pseudoprimes and Carmichael Numbers" that not only are there infinitely many Carmichael numbers, but they aren't as rare as one might expect.

Conjecture 1. *Let $C(x)$ denote the number of Carmichael numbers $\leq x$. For each $\varepsilon > 0$, there exists a number $x_0(\varepsilon)$ such that $C(x) > x^{1-\varepsilon}$ for all $x \geq x_0(\varepsilon)$.*

What does this conjecture mean? It is important that this is a statement for *each* $\varepsilon > 0$, including extremely small ones. Thus, $x^{1-\varepsilon}$ can be close to x. Fortunately, for large x, $x^{1-\varepsilon}$ becomes farther from x, even if ε is quite small.

As explained earlier, a primality test is only useful if it can be executed in polynomial time. The Fermat test involves calculating b^{n-1} modulo n for various bases b. You might expect that this calculation would take a long time because it would involve $n-2$ multiplications. However, we can use an algorithm called *fast modular exponentiation* instead of naïvely multiplying. This algorithm can be done in polynomial time in the number of binary digits, as hoped, specifically, its running time when calculating $a^b \mod n$ is $O((\log_2 b)(\log_2 a)^2)$.

Let's illustrate this algorithm by calculating $3^{900} \mod 39$. Write 900 in its binary form, 1110000100. We loop through the binary digits of 900. We start with $c = 1$. For each binary digit, we update c to c^2. If the digit is a 1, then we also update c to $3c$. In each step, we reduce modulo 39.

$i = 0$	$c = 1^2 = 1$	$c = 1 \cdot 3 = 3$
$i = 1$	$c = 3^2 = 9$	$c = 9 \cdot 3 = 27$
$i = 2$	$c = 27^2 = 729 \equiv 27$	$c = 27 \cdot 3 = 81 \equiv 3$
$i = 3$	$c = 3^2 = 9$	
$i = 4$	$c = 9^2 = 81 \equiv 3$	
$i = 5$	$c = 3^2 = 9$	
$i = 6$	$c = 9^2 = 81 \equiv 3$	
$i = 7$	$c = 3^2 = 9$	$c = 9 \cdot 3 = 27$
$i = 8$	$c = 27^2 = 729 \equiv 27$	
$i = 9$	$c = 27^2 = 729 \equiv 27$	

We found that $3^{900} \equiv 27 \mod 39$ in only 10 steps, the number of binary digits in 900. This algorithm for calculating $a^b \bmod n$ takes up to $\log_2 b$ steps. Each step is multiplication, so it is $O((\log_2 a)^2)$. Therefore, overall, modular exponentiation is $O((\log_2 a)^2(\log_2 b))$. This means that the Fermat test is $O((\log_2 n)^3)$, since we use b's that are less than n.

In summary, when looking for a large prime number, one option is to randomly pick a large number n and test to see if it is prime using the Fermat Primality Test. That is, first pick a base b such that $\gcd(b, n) = 1$, which can be checked using Euclid's algorithm. Then check whether $b^{p-1} \equiv 1 \mod p$ using fast modular exponentiation. If n passes the test for many bases, it is highly likely that it is prime. However, there are infinitely many pseudoprimes for each base, and there are infinitely many composite numbers that will pass every test. The only way to test to see if a large number is a Carmichael number would involve years of computation since it requires the prime factorization of both n and $n - 1$. Fortunately, the probability that n is a Carmichael number is extremely low.

More sophisticated tests, such as the Euler Quadratic Reciprocity Test and the Miller-Rabin Test, have been developed that depend on other properties of prime numbers and do not have the problem of Carmichael numbers. However, these tests are all probabilistic tests and thus do not prove that a number is prime.

3.3. AKS Test

Until 2002, any deterministic test was far too inefficient to be practical. However, in 2002, a deterministic test was discovered that can test whether or not a number is prime in polynomial time. It was discovered by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena and is called the AKS algorithm. Again, their test is based on a property of prime numbers. However, this property is only a property for prime numbers. Thus, we will not find any pseudoprimes. Also important is that we can quickly check that a number has this property.

We need to make a few quick comments before stating the property. A number n is a perfect power if $n = a^k$ for integers a and k. We will make the statement $(x+a)^n \equiv x^n + a \mod (n, x^r - 1)$. This is a polynomial congruence modulo $(n, x^r - 1)$, so it is referring to two polynomials in x being equivalent, not saying that this statement is true for every value of x. What does that mean? Two polynomials $h(x)$ and $g(x)$ with integer coefficients are congruent modulo n and $x^r - 1$ if and only if there exist polynomials with integer coefficients $u(x)$ and $v(x)$ such that $f(x) - g(x) = nu(x) + (x^r - 1)v(x)$. Considering a polynomial modulo $x^r - 1$ means that $x^r \equiv 1$, so the degree of the polynomial can be limited to r.

Theorem 19. *Let $n > 1$ be an integer. Let $r < n$ be an integer such that the order of n modulo r is greater than $(\log_2 n)^2$. Then n is prime if and only if*

1. *n is not a perfect power,*
2. *n does not have a prime factor $\leq r$,*
3. *$(x+a)^n \equiv x^n + a \mod (n, x^r - 1)$ for each integer a such that $1 \leq a \leq \sqrt{r} \log_2 n$.*

The proof of this theorem is elementary, but it requires much Abstract Algebra. If you would like to read it, a good source is Granville's paper "It is Easy to Determine Whether a Given Integer is Prime."

Since this property is only a property of prime numbers, we do not need to consider pseudoprimes. However, we need to check that it can be tested in polynomial time. It can be shown that this algorithm is $O((\log_2 n)^{7.49})$ and that slight improvements can be made by altering the algorithm. Please refer to Granville's paper for details.

4. RSA Encryption

We have seen various ways to find prime numbers. We conclude with an application for these primality tests. Suppose that you want to send a secret message to your friend. You need to secretly tell your friend how to read it, right? But then how do you send *that* secret information? Traditionally, a cryptosystem, or method for encrypting and decrypting messages, has involved communicating a "private key" to the person who wants to decrypt the message. In 1976, Whitfield Diffie and Martin E. Hellman proposed the idea of a public key cryptosystem. In this system, each sender would have a public encryption key and a private decryption key. Suppose Alice wants to send a message to Bob. She uses his public encryption key and sends him the message. Bob is the only person who can read it because he has his private decryption key. It would be crucial in this system that Bob's private decryption key cannot be determined from his public encryption key. This involves using a "trapdoor one-way function."

Definition 10. Let S and T be finite sets. A *trapdoor one-way function* $f : S \to T$ is an invertible function satisfying:

1. Given $x \in S$, $f(x) \in T$ is easy to compute.
2. Given $y \in T$, $f^{-1}(y) \in S$ is difficult to compute.
3. f^{-1} is easy to compute if one has secret information (a trapdoor).

(Yan 348-352).

The first people to find a practical public key cryptosystem were Ronald L. Rivest, Adi Shamir, and Leonard Adleman in 1978. Their public-key system is the RSA algorithm previously mentioned.

We now describe this algorithm in detail. Let's call the original message, the plaintext, M and the encrypted message, the ciphertext, C. How does Alice create C from M in order to send a secret message to Bob? First, Bob finds two large prime numbers, p and q. He sets $N = pq$. He then picks e, the public encryption exponent, so that $\gcd(e, \phi(N)) = 1$. Next he calculates d, the private decryption exponent, by $d \equiv 1/e \mod \phi(N)$, so that $ed \equiv 1 \mod \phi(N)$. We know that such a d exists by Theorem 7. He publishes e and N, keeps d secret, and destroys all evidence of p and q. Then, Alice finds the ciphertext C by setting

$$C \equiv M^e \mod N.$$

Bob receives this ciphertext and reads it by setting

$$M \equiv C^d \mod N.$$

We will illustrate this system with an example. We will use the same p, q, e, and d as an example in Yan's *Number Theory for Computing*. Suppose that Notre Dame's Athletic Director, Jack Swarbrick, wants to give the University President Fr. Jenkins the secret news that Brian Kelly accepted the offer to be Notre Dame's new head football coach. Suppose Fr. Jenkins is prepared to receive secret messages. He randomly chose the primes $p = 71593$ and $q = 77041$ using a primality test such as the Fermat test. He calculated $N = 71593 \cdot 77041 = 5515596313$ and $\phi(N) = (71593 - 1)(77041 - 1) = 5515447680$. He chose a public encryption exponent, $e = 1757316971$ after checking that $\gcd(e, N) = 1$ using Euclid's algorithm. He then calculated his secret decryption exponent, $d \equiv 1/e \equiv 2674607171 \mod \phi(N)$ (Yan 360). Fr. Jenkins published e and N, put d in a secret place, and destroyed the evidence of p and q. Now that Swarbrick has news, he can encrypt his message "BRIAN KELLY IS NEW COACH."

First Swarbrick needs to rewrite his message in numbers. He replaces each space with 00, each A with 01, and so forth, through replacing Z with 26. He also breaks his message into blocks of 10 numbers, padding the front with zeros if necessary. Thus, his message becomes

0002180901 1400110512 1225000919

0014052300 0315010308

Swarbrick then uses fast modular exponentiation to evaluate each block raised to the e^{th} power modulo N. Each of the following equations will be considered modulo 5515596313.

$$(0002180901)^{1757316971} \equiv 2574007107$$
$$(1400110512)^{1757316971} \equiv 1327543223$$
$$(1225000919)^{1757316971} \equiv 1961557673$$
$$(0014052300)^{1757316971} \equiv 4632175637$$
$$(0315010308)^{1757316971} \equiv 0144453518$$

He is now ready to send his message to Fr. Jenkins:

$$257400710713275432231961557673$$

$$46321756370144453518\,.$$

Fr. Jenkins is the only person who can read this message because only he has the private key d. He breaks the message back up into blocks of 10 and uses fast modular exponentiation to evaluate each block to the d^{th} power modulo N. Again, each of the following equations will be considered modulo 5515596313.

$$\begin{aligned}
(2574007107)^{2674607171} &\equiv 0002180901\\
(1327543223)^{2674607171} &\equiv 1400110512\\
(1961557673)^{2674607171} &\equiv 1225000919\\
(4632175637)^{2674607171} &\equiv 0014052300\\
(0144453518)^{2674607171} &\equiv 0315010308
\end{aligned}$$

Fr. Jenkins can then write his whole message as

$$000218090114001105121225000$$

$$91900140523000315010308\,.$$

This is the same sequence of numbers listed above just after Swarbrick translated his message into numbers. As one last step, Fr. Jenkins translates these numbers back into letters. He recovers the secret message "BRIAN KELLY IS NEW COACH" and smiles as he watches the press attempt to get the scoop.

First, why is Fr. Jenkins successful in recovering M? Recall that $ed \equiv 1 \mod \phi(N)$. This means that $ed = k\phi(N) + 1$ for some $k \in \mathbb{Z}$. Then we can write

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k\phi(N)+1} \equiv (M^{\phi(N)})^k M$$

$$\equiv (1)^k M \equiv M \mod N\,.$$

So, we can see why Swarbrick is successfully able to send a message to Fr. Jenkins this way.

Why does the message remain secret? At first glance, you may say that of course only Fr. Jenkins can read the message because only he knows d. However, you want to be confident that this message is truly secret. After all, we want to be sure that the football players and the university's top donors hear of the new hire from Fr. Jenkins personally, not from some reporter on ESPN (or perhaps you are concerned about the security of your credit card.) You begin to worry. The general public can access both e and N. Could someone calculate d from that information?

Recall that d was calculated as $d \equiv 1/e \mod \phi(N)$. This seems alarming. The public knows e and N. Anyone could do a quick web search and find out how to calculate $\phi(N)$. However, $N = pq$ for two very large secret prime numbers. Suppose a news reporter, Eve, knows N and the formula for $\phi(N)$. In order to calculate $\phi(N)$, she first needs to find the prime factorization of N. As mentioned previously, the security of RSA relies on the fact that prime factorization is a very difficult problem. There is no sufficiently fast way to find p and q from N, so Eve is stuck and there is no leak to the press.

How difficult is integer factorization? Andrew Granville describes in his article "It is Easy to Determine Whether a Given Integer is Prime" the difficulty of factoring a 400 digit number, the product of two 200 digit primes, as "beyond practical reach," where "practical reach" is defined as "using all computers that have or will be built for the next century, assuming that improvements in technology do not happen much faster than we have seen in the last couple of decades (during which time computer technology has, by any standards, developed spectacularly rapidly)" (4).

Are there other ways to decrypt messages besides factoring N? This is an area of continuing research. The RSA Conjecture is that any method of breaking RSA must be as difficult as factoring (Yan 372). For a more detailed discussion of the possible attacks, see Dan Boneh's article "Twenty Years of Attacks on the RSA Cryptosystem."

Remember that Diffie and Hellman suggested that a public key cryptosystem could work if it was based on a one-way trapdoor function. RSA indeed is based on such a function. It is easy to find two prime numbers and compute $M^e \mod N$. It is difficult to compute $C^{1/e} \mod N$ without knowing the factorization of N or $\phi(N)$. Fr. Jenkins has the trapdoor, but the rest of the world does not (Yan 358-360).

5. Conclusion

Prime numbers have been studied for thousands of years with no application in mind. In 1801, the great mathematician Gauss stated,

> The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and difficult that even for numbers that do not exceed the limits of tables constructed by estimable men, they try the patience of even the practiced calculator. . . Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

With the realization of the application of primality tests about forty years ago, this question grew from a matter of mathematical curiosity to a matter of information security. We have discussed several primality tests. The AKS algorithm is significant because it finally provides what Gauss was looking for, a computationally feasible way to know for sure whether or not a large number is prime. We have also discussed how the RSA cryptosystem works and its reliance on prime numbers.

Works Cited

Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. "PRIMES is in P." *Ann. of Math.* 2nd ser. 160 (2004): 781-93. Print.

Boneh, Dan. "Twenty Years of Attacks on the RSA Cryptosystem." *Notices of the AMS* 46 (1999): 203-13. Print.

Crandall, Richard, and Carl Pomerance. *Prime Numbers: A Computational Perspective*. New York: Springer, 2005. Print.

Erdős, Paul. "On Almost Primes." *Am. Math. Mon* 57 (1950): 404-07. Print.

Erdős, Paul. "On Pseudoprimes and Carmichael Numbers." *Publ. Math. Debrecen* 4 (1956): 201-06. Print.

Granville, Andrew. "It is Easy to Determine Whether a Given Integer is Prime." *Bull. Amer. Math. Soc.* 42 (2004): 3-38. Print.

Koblitz, Neal. *A Course in Number Theory and Cryptography.* New York: Springer, 2006. Print.

"RSA Laboratories - The RSA Challenge Numbers." *RSA, The Security Division of EMC: Security Solutions for Business Acceleration*. Web. 05 Mar. 2010.

Yan, Song Y. *Number Theory for Computing*. Berlin: Springer, 2002. Print.

The author acknowledges the guidance of Prof. D. Galvin, Ph.D., Department of Mathematics, in writing her senior thesis, part of which has been used to generate this article.

The Effect of Urbanization on Bird Foraging

David J. Chan and Regina M. McCormack
Advisors: Erica Kistner and Dom Chaloner, Ph.D.
University of Notre Dame, Department of Biological Sciences

Abstract

Urbanization due to human population growth affects floral and faunal populations. Foraging studies, such as giving up densities (GUDs), indicate the effects of urbanization. GUD is higher in areas of low foraging and lower in areas of high foraging. Foraging intensity is affected by three factors: the energy exerted while foraging, the missed opportunity costs, and the perceived risk of predation. The effects of these factors are demonstrated in the GUD. This study examined GUDs of birds on the University of Notre Dame campus, both in a forested environment and in an urban environment. We hypothesized that the birds would exhibit a lower GUD in the urban environment and a higher GUD in the natural environment. Surprisingly, the results indicate that GUD is lower in forested environments, suggesting that birds perceive a greater risk of predation in urbanized areas due to lack of protective cover. Furthermore, analysis of data during precipitation events supports the hypothesis that foragers perceive a lesser threat of predation when foraging in the rain. These results imply that urbanization affects local ecosystems, thus warranting careful consideration of both urban planning and conservation management.

Introduction

As the human population grows, land use is inevitably shifting toward urban landscapes (1). For example, urban land in the United States increased by 9 million acres between 1960 and 1970 and then increased by 13 million acres between 1970 and 1980 (2). Along with the conversion of land to high density population centers comes the destruction of natural habitats. Urbanization thus dramatically alters floral and faunal populations. Foraging studies can measure the extent of this alteration as a number of inputs affect organisms' foraging habits (3). By comparing the foraging habits of organisms in an urban area with those of a more natural environment, the anthropogenic effect can be quantified to better understand the impact of urbanization on ecosystems.

A common feature examined in foraging studies is an organism's giving up density (GUD). Essentially, GUD is the density of resources in a food patch when foraging stops. The basis of GUD is the marginal value theorem from economics, in that, in accordance to optimal foraging theory, a forager should stay in a resource patch as long as the energy gain balances the costs of foraging (4). Brown (5) defined the costs of foraging as three-fold: the cost of exerted energy, the cost of missed opportunity, and the cost of perceived predation risk.

One of the costs of foraging, the cost of exerted energy, motivates organisms to optimize their foraging efforts. Foragers will spend time feeding at a site if the food source will provide more energy than they must expend to retrieve it. Consequently, organisms will not spend time feeding when the food will yield less energy than they expend. This effort to maximize energy gained per unit energy spent is called the optimal foraging theory (4, 6, 7). Behavior due to the optimal foraging theory is revealed in GUDs. Foragers who do not believe they will maximize the energy gained from a food source will leave a high GUD, while foragers who maximize energy at a site will leave a low GUD (6, 7).

Another cost of foraging, the missed opportunity cost, is related to the optimal foraging theory. Foragers are constantly searching for more efficient, alternative food sources. If one area contains several food patches, the forager has many opportunities to forage. When a forager decides to feed in one area, the other available food patches become missed opportunities. The potential benefits of foraging at these alternative food patches amount to missed opportunity costs (5, 6). Generally, when the missed opportunity costs increase, the GUDs increase as well (5, 6). Foragers do not spend as much time feeding in one place because they move to different patches, making sure they are acquiring optimal resources. Thus, foragers' attempts to take advantage of opportunities are revealed in the GUDs. Places that contain many different sites to forage will generally have high missed opportunity costs and therefore high GUDs.

Vital resource abundance is a factor that alters the effects of the optimal foraging theory and missed opportunity costs. Abundances of resources other than food, such as water, can motivate foragers to behave in certain ways. Foragers may feel more comfortable foraging in areas with readily available water and thus feed longer, leaving low GUDs. Consequently, a lack of water may stress individuals, prompting them to spend more time searching for water and less time feeding in one area, producing high GUDs. Shochat et al. (6) examined GUDs of birds in Arizona in a natural, desert environment and in an urbanized environment. They determined that the GUDs of

birds in urban environments were lower (6). The researchers speculated that water resources may have been more plentiful in the urban environment, so birds may have been more inclined to spend their time feeding in the urban environment, leaving low GUDs. Birds in the desert may have had to move from feeding site to feeding site to ensure access to water, thus leaving high GUDs. Thus, resource abundance is a factor to consider when examining behavior due to the optimal foraging theory and the number of missed opportunity costs.

While the exerted energy cost and the missed opportunity costs account for the foragers' response to its food source, the predation risk cost accounts for the foragers' relationship with the other organisms in its environment. Foragers are constantly aware of predators, and they will not spend time feeding in area if they sense predators nearby. GUDs will be high when foragers perceive an eminent predator threat. When foragers do not sense predators, they will forage until they are satiated in one area, thus generating a low GUD (3). For example, researchers in Virginia examined the GUDs of gray squirrels (Sciurus carolinensis) in natural and urban environments and attributed the difference to the abundance of predators in each environment. The urban environment, which had fewer natural predators, yielded the lower GUD (3).

Though foragers will flee when they perceive a predation threat, they may be swayed to stay at a feeding site if the microhabitat effectively obscures them from predators. Thus, microhabitat may also affect foragers' GUDs (8). In a study of the foraging behaviors of rodents in South Carolina, rodents had lower GUDs in areas with vegetation cover and during precipitation events (8). The vegetation cover obscured the foragers from predators, and the precipitation lessened the predators' clarity of vision and thus ability to detect foragers (8). The rodents' reactions to the urine scents of predators were also tested and were found to have less of an impact on the GUDs than the microhabitat features (8). Another factor of microhabitat is the distance between the foraging area and protective shelter. A study in Israel examined sparrows' (*Passer spp.*) feeding behavior and determined that the GUD increased when the foraging area's distance from shelter increased (7). The sparrows perceive the greater distances between their shelter and their food source as an elevated threat. The longer the bird is in flight, the more visible it is to predators. These studies demonstrate that the threat of predation is a constant factor affecting foragers' decisions.

The Notre Dame campus provides a good setting to study the effects of urbanization on the local fauna. This study contrasts the GUDs of birds in both a forested area and the urban setting to elucidate these effects. The hypothesis is that birds will have a lower GUD in the urban environment and a higher GUD in the natural environment as a function of a lower perceived predation risk, lower resource abundance, and fewer missed opportunity costs in an urban environment. A second hypothesis is that birds will have a lower GUD during precipitation events because the precipitation alters the microhabitat, reducing the predators' visibility and thus obscuring the foragers from view.

Methods

The research sites were located on the campus of the University of Notre Dame. Originally five feeding stations were randomly placed both on the northern side of the campus (Fig. 1), representing an urban environment, and in a woodlot adjacent to the campus, representing a forested environment. The two environments were ~0.5km apart. Due to vandalism, three of the feeders in the woodlot were destroyed early in the experiment, so one feeder was moved from the urban environment to the woodlot. With three feeders in the natural environment and four feeders in the urban, the replication was adjusted so that nineteen replicates were taken from the urban

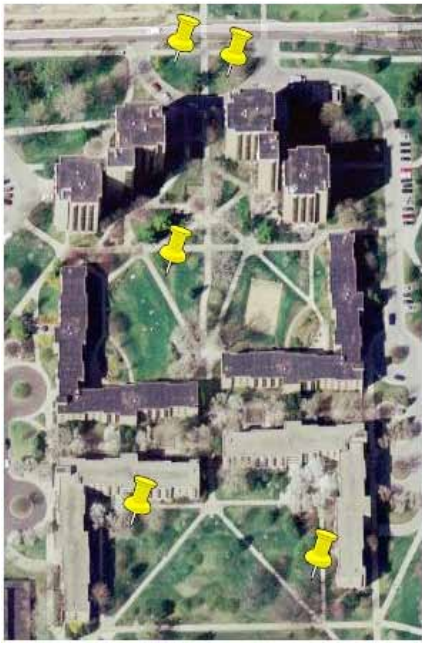


Figure 1. Location of the urban study sites on the Notre Dame campus. These sites are disturbed by pedestrian and automotive traffic. Image courtesy of Google Earth®.

environment and seventeen replicates were taken from the natural environment.

Custom-built bird feeders (Fig. 2) based on the feeders used in Bowers and Breland's study (3) were used for the feeding stations in this study (see figure legend for detailed description). To discourage squirrels from getting into the feeders, a plastic funnel was placed halfway up the pole of each of the feeders to act as a squirrel baffle. Additionally, the PVC pipe, the pole, and the baffle were greased with Crisco© shortening and covered with chili powder to further deter the squirrels. These tactics were successful because no evidence of squirrel activity was observed.

Figure 2. **Bird feeder used in the study,** *consisting of a 1.2m rake handle on which was mounted an aluminum pie dish (0.23m diameter, 0.05m deep). The base of the feeder consisted of a ~0.4m length of PVC pipe to allow for easy feeder removal, surrounded by crushed limestone in a plastic flower pot to keep the feeder upright. A plastic funnel was placed halfway up the pole of each of the feeders to act as a squirrel baffle. Additionally, the PVC pipe, the pole, and the baffle were greased with Crisco© shortening and covered with chili powder to further deter the squirrels.*

The experiment was run from 1 November-16 November 2009, a period of typically cool yet sunny Midwestern autumn days with occasional rain. Feeders were set out with wild bird seed mix for a one week habituation period, thereby giving time for the birds to get used to feeding from them. After the habituation period, the feeders were filled with 5g safflower seed mixed with 0.5L dry sifted sand (density substratum), giving the feeders a baseline density of 10g/L. Safflower was used because it is a common seed used for birds of the Indiana area, and squirrels do not like to eat it (Wild Birds, Unlimited, personal communication). The sand/seed mixture was allowed to stay out for a 24hr period before being collected and analyzed in the lab. The experiment ran for a week, with the sand/seed mixture in each feeder being collected and replaced with 0.5L of the sand/seed mixture daily. The samples collected from the feeders were sifted to remove the sand and had their empty seed shells removed by hand. If it had rained while the sample was out, the sample was dried overnight in a 100°C oven prior to being sifted. The remaining safflower seed was weighed to obtained the final seed mass, which was divided by 0.5 to obtain the final density in each patch. The data was analyzed for normal distribution using a Shapiro-Wilk test on MYSTAT 12. Because the data was normally distributed (p-value=0.690), ANOVAs were performed to determine both the site's effect and the precipitation's effect on the final density. A regression analysis was performed to determine if the GUDs changed over time.

Results

An ANOVA of final density and site revealed that forested sites had a significantly lower GUD (=6.545 ± SE 0.299 g/L) than the GUD of urban sites (=7.582 ± SE 0.273 g/L) (F1,34=6.423, p=0.016) (Fig. 3). During the experiment, there were days in which it rained, giving 13 rain samples and 23 samples with no rain. With an ANOVA, it was found that samples taken from when it rained had a significantly lower GUD (=5.863 ± SE 0.324 g/L) than when it did not rain (=7.697 ± SE 0.18 g/L) (F1,34=29, p=5.4x10-6). Further breakdown of the data using ANOVA tests revealed no statistically significant difference between the sites during rain events (F1,11=2.39, p=0.15), while analysis of variance in the data from only the rainless days maintained

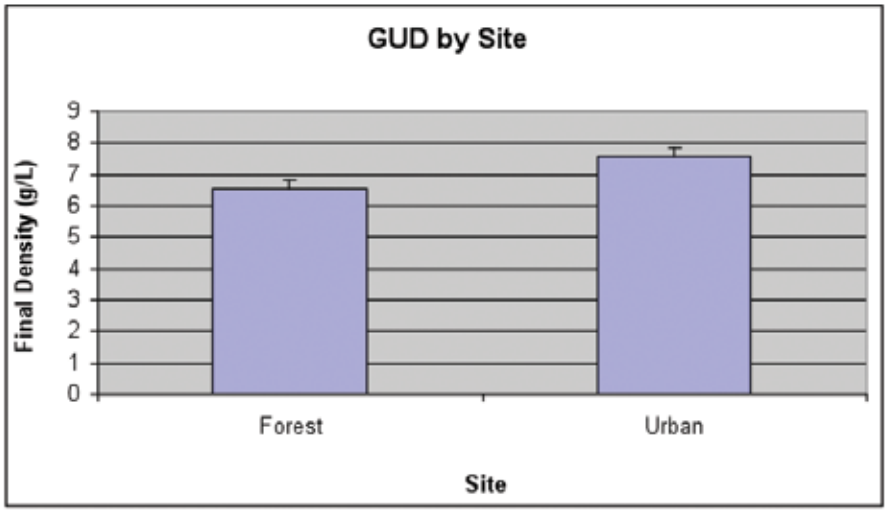


Figure 3. **Mean final density of each site type.** *Final density is assumed to correspond to GUD. Forested sites had a significantly (F1,34=6.423, p=0.016) lower GUD than urban environments.*

the lower GUD in the forests (=7.313 ± SE 0.239 g/L) than in the urban environment (=8.048 ± SE 0.231 g/L) (F1,21=4.889, p=0.038) (Fig. 4). Regression analysis of final density for the two sites over time yielded no statistically significant correlation between final density and date of collection (forest: R^2= 0.085, p=0.226; urban: R^2= 0.015, p=0.650).

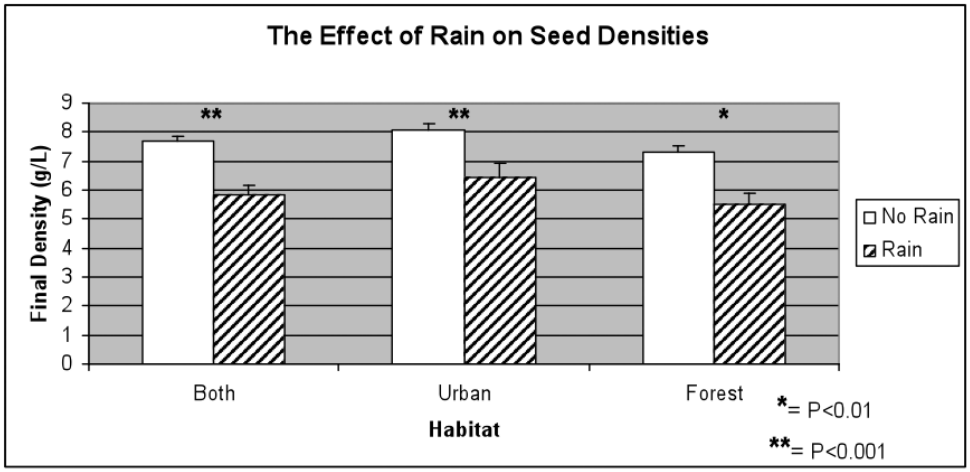


Figure 4. **Effect of rain on GUD.** *When it rained, there was a statistically significantly lower GUD than when it didn't (F1,34=29, p=5.4x10-6). This holds true for both the forested habitat alone (F1,17=17.19, p=6.8x10-4) and the urban habitat alone (F1,15=11.604, p=0.004).*

Discussion

Contrary to our original hypothesis, our data does not indicate that the GUD of birds in the urban environment is lower than the GUD of birds in a forested environment. Rather, it suggests the opposite conclusion. This result seems to contradict a previous study that found gray squirrels to have a lower GUD in an urban environment than a forested environment (3). The explanation for this difference is reflected in several studies that suggest a lower predation risk (or a lower sensitivity to such as risk) for foragers in an urban environment (3, 7, 9).

Anthropogenic Inputs

In consideration of the perceived risk of predation, these results indicate that birds may perceive predation as a greater risk in the urban environments. Perhaps birds may perceive humans to be a greater threat than other natural predators. Alternatively, the disturbance of human activity associated with the urban environment, such as light and noise pollution (10, 11), may deter birds from feeding in areas for extended periods of time. The disturbance of urban environments is quite frequent. Vehicles speed down roads regularly, and people are often walking outside. These disturbances produce more physical activity and greater noise levels than those found in natural environments. Even though there may be fewer natural predators in the urban environment, the high frequency of disturbance may deter birds from feeding, thus affecting the GUD.

Study System

Another explanation for the unexpected low GUD of the natural environment is the possibility that there is little significant difference in the number of predators in the urban and natural environments used in this study. The Notre Dame campus is more suburban than urban, so it contains trees and other vegetation that could potentially house predators as well as birds. Additionally, the woodlot used in this study is very small (<0.5km2) and surrounded on all sides by urban development. If these two sites were placed on an urbanization gradient, they would fall close together rather than far apart on polar ends of the spectrum, which may be the reason why such a low difference in mean GUD between the sites (~1g/L) was seen. Also, the distance between the urban and natural environments on the Notre Dame campus is approximately one half kilometer. Perhaps this distance is too short to cause a significant difference in abundance of predators in the urban and natural environments. If there is no significant difference, then perhaps anthropogenic disturbance is the primary factor affecting bird GUD.

Effect of Microhabitat

Although abundance of predators and frequency of disturbance affect GUDs, the characteristics of the microhabitat also are fundamental factors that determine bird GUDs. A rodent study in South Carolina found that rodents had higher GUDs in full moonlight and in open areas. In contrast, the rodents left lower GUDs in areas with low light and dense vegetation, showing that rodents prefer to feed in areas that would effectively conceal them from predators (8). Though rodents and the birds in our study belong to different taxonomic groups, they both fall within the granivore feeding guild and thus may exhibit similar foraging habits (12).

In the Notre Dame study, protective microhabitat may have been the driving factor affecting GUDs. The forest provides many tree branches, leaf clus-

ters, bushes, fallen logs, and piles of leaf litter that constitute a dense framework of protective shelters, while shelter in the urban environment was much more sparse. Non-urban birds were found to exhibit a GUD gradient based on distance to shelter, with closer food patches having a lower GUD than farther patches (7). Although this study did not find such a gradient for the species of urban birds they used, such a gradient could potentially exist for our study and the greater abundance of shelter in the forest could explain why it had a lower GUD.

Another potential explanation for the trend seen is that there may be a greater number of birds in the forest. This would cause increased competition for the limited food resource. In this high competition environment, in order to get enough food, birds cannot afford to leave a high density of food as they would in a low competition environment. This causes the GUD to be lower. However, because the urban and natural environments are only approximately one half kilometer apart and the urban environment contains trees and other nesting points, the possible difference in the density of birds should not be considered the primary explanation without further study.

Rain

Our rain results support the findings of a previous GUD study on old-field mice (Peromyscus polionotus), which also found a lower GUD in the rain. In this case, the rain was considered an indirect cue of a lower predation risk from multiple predators, as it can lower a predator's ability to detect prey (8). The lack of differences between the sites in the rain may stem from urban and forest birds reacting equally to the rain. A small sample size of rain data could also have led to non-significant differences between the sites. Although the p-value was non-significant (0.15), there was a trend toward the forested sites having lower GUDs than the urban sites, as was the case with the non-rain data.

Implications of Urbanization

Foraging studies are a useful metric of measuring habitat preference, predation risk, and competition in an area (5). From a conservation/management perspective, studies such as ours are important in that they can be used as an indicator of anthropogenic impact on an area or population (3). This has implications for practices such as threatened species recovery. By knowing how impacted an area is, managers can choose to focus recovery efforts on areas they know have little human impact, potentially giving the threatened species a better chance of bouncing back. Additionally, studies on the effects of urbanization are important to try to predict how a population will react to urbanization and whether or not it could drive them to extinction.

The effects of urbanization often yield detrimental ecological effects. Studies have shown that human-induced noise levels in particular interfere with birds' communication and thus reproduction (11, 13). Urbanization often deters bird reproduction, leading to decreased density and diversity of bird populations over large geographical areas (13). Another potential result of urbanization is eventual speciation. Birds that forage in the forest undergo natural selection by their ability to avoid predators. In the urban environment where there are fewer predators, birds may be selected for competitive advantage rather than superior ability to avoid predators. Birds in urban environments may encounter competition for resources, so those who will survive will be those with superior traits for acquiring resources. The different demands of the different environments may lead to eventual speciation.

Conclusion

Although this study produced significant results, they contrasted with results in earlier scientific literature. This contradiction warrants the need for future study of the effect of urbanization on GUD. This study may be improved before further implementation. Because the Notre Dame campus is more suburban than urban, sampling from three different environments, an urban, a suburban, and a natural, may yield more accurate results. Also, using camera traps at each feeding site would enable researchers to know the numbers and species of birds that eat from the feeders and thus aid researchers with analysis. If the density of the birds of the two environments is significantly different, then the GUD cannot be considered a true measure of birds' perceived risk of predation. The various preferences and behaviors of different species of birds may also affect the GUD. Although most birds native to the Midwest eat safflower seeds, perhaps a few species do not prefer them. Identifying the birds that feed at the birdfeeders may enable researchers to explain any potentially perplexing data.

As our study shows, there is an impact by urbanization on the foraging habits of local fauna. Though this study reveals different results than what is known from the literature in other ecosystems, more extensive studies need to be done for this area's ecotype to determine the actual magnitude of

urbanization on the local ecosystem. If this study is exemplary of birds' foraging habits in Indiana, then it shows that birds thrive most strongly in their non-urbanized environments. Thus, it is important for both conservationists and urban planners to strive to maintain an environment that can support both human populations and the biodiversity of local fauna. Knowing how humans affect the environment enables humans to take action against potential ecological damage. Using measures such as GUDs serve as instruments aid scientists in achieving these goals.

Acknowledgements
We would like to thank the University of Notre Dame's Department of Biology for funding this project and allowing it to be conducted. We would also like to thank Patrick McCauslin in Landscape Services for granting approval to conduct the research on campus, as well as supplying some of the materials for the feeders. And finally, we would like to thank Dom Chaloner, Ph.D., Erica Kistner, and Chelse Prather for constructing the feeders, purchasing materials for the study, and offering their guidance throughout the duration of this project.

Literature Cited

1. McDonnell, M. J. and S. T. A. Pickett. 1990. Ecosystem structure and function along urban-rural gradients: An unexploited opportunity for ecology. *Ecology* 71:1232-1237

2. Frey, H. T. 1984. Expansion of urban area in the United States: 1960-1980. United States Department of Agriculture Economic Research Service Staff Report Number AGES830615

3. Bowers, M. A., and B. Breland. 1996. Foraging of gray squirrels on an urban-rural gradient: Use of GUD to assess anthropogenic impact. *Ecological Applications* 6:1135-1142

4. Charnov, E. L. 1976. Optimal foraging, the marginal value theorem. *Theoretical Population Biology* 9:129-136

5. Brown, J. S. 1988. Patch use as an indicator of habitat preference, predation risk, and competition. *Behavior Ecology and Sociobiology* 22:37-47

6. Shochat, E., S. B. Lerman, M. Katti, and D. B. Lewis. 2004. Linking optimal foraging behavior to bird community structure in an urban-desert landscape: Field experiments with artificial food patches. *The American Naturalist* 164:232-243

7. Tsurim, I., Z. Abramsky, and B. P. Kotler. 2008. Foraging behavior of urban birds: Are human commensals less sensitive to predation risk than their nonurban counterparts? *The Condor* 110:772-776

8. Orrock, J. L. and B. J. Danielson. (2004). Rodents balancing a variety of risks: Invasive fire ants and indirect and direct indicators of predation risk. *Oecologia* 140:663-667

9. Shochat, E. 2004. Credit or debit? Resource input changes population dynamics of city-slicker birds. *Oikos* 106:622-626

10. Longcore, T. and C. Rich. 2004. Ecological Light Pollution. Frontiers in Ecology and the Environment 2:191-198

11. Francis, C. D., C. P. Ortega, and A. Cruz. 2009 Noise pollution changes avian communities and species interactions. *Current Biology* 19:1415-1419

12. Simberloff, D. and T. Dayan. 1991, The guild concept and the structure of ecological communities. *Annual Review of Ecology, Evololution, and Systematics* 22:115-143

13. Slabbekoorn, H. and E. A. Ripmeester. 2008. Birdsong and anthropogenic noise: implications and applications for conservation. *Molecular Ecology* 17:72-83

From Statistics to Particles in Quantum Mechanics

Kristina Sault

University of Notre Dame, Department of Physics

Abstract

The character of quantum particles is considered by route of what we know of classical and quantum statistics. The presentation is given in terms of classical statistics and bosonics statistics, but familiar extension shows that the conclusions are entirely general to the quantum realm. In this paper, we examine the widespread belief that quantum statistics are entirely due to the indistinguishibility of quantum particles. In the accompanying paper we, we modify this claim and show that not only the indistinguishibility of particles but also discrete quantum mechanical states and a precise quantum mechanical measure are required for quantum statistics.

I. INTRODUCTION

Quantum mechanics bloomed with the explanation of spectra; Planck's of the spectra of black-body radiation and Pauli's of the elements subject to strong magnetic fields. With his quantum of action, h, Planck averted the ultraviolet catastrophe. With his Exclusion Principle, Pauli reduced "the complicated numbers of electrons in closed subgroups [to] the simple number one." [1] The distributions they studied characterize two separate classes which partition the elementary constituents of nature into bosons and fermions.

The names we adopt for these classes admit that we speak of particles. This is an assumption, but one which appears natural in quantum mechanics. There is some contention over whether particles can be called classical. For our purposes, a classical particle is body which exists somewhere between our recognition that it is convenient to talk of a discrete number of bodies, such as a mole, and the full revelation of quantum mechanics.

In the following we investigate the nature of quantum particles with powerful tools: classical particles, their Maxwell-Boltzmann distribution, and the bosons' Bose-Einstein distribution. Along the way we discover that we must understand our investigation before we can understand the quantum.

II. BLACKBODIES AND THE EXCLUSION PRINCIPLE

Blackbodies are objects which absorb all incident radiation of any wavelength. When in equilibrium, blackbodies emit as much as they absorb. Thus a cavity made of blackbody material will contain a gas of photons. The gas exhibits a spectral energy density; Planck was the first to describe this consistently with his formula

$$u(\omega) = \frac{\omega^2}{\pi^2 c^3} \quad \frac{\hbar\omega}{e^{-\beta\hbar\omega} - 1} \tag{1}$$

As we will see below this is a particular case of the Bose-Einstein distribution.

Pauli's exclusion principle explains the distribution of electrons over available quantum states. Realizing that energy levels can be degenerate, he discovered that with a full description of states any one of these can accomadate at most a single electron. In general this is true for any fermionic state; with occupation numbers $\{0, 1\}$, they are either empty or full.

We can derive such a set of occupation numbers from the black-body distribution Equation 1. Inductive reasoning proves fruitful, for the answer is well-known. A careful approach to the result reveals what we can say and what we should not assume about bosons.

III. OCCUPATION NUMBERS

First we must choose a sensible system to massage. The realization of occupation numbers depends on particle number, for it is particles which do the occupying. Thus we should not restrict our particle number or we might artificially limit the possible occupation numbers. Adopting particle number as a degree of freedom, we should also allow the energy of our system to vary, for the total energy of a system is related to the number of particles it has. Such a system is a grand canonical ensemble; it can remain in equilibrium while exchanging particles and energy with a limitless reservoir. Below we review the common textbook presentation of a grand canonical ensemble. [2] [3] Our presentation is intentionally succinct; it masks assumptions that we will later explore in depth.

It is convenient to relate the energy of a particular state of the system directly to its numbers of particles, so the energy of the k^{th} state, say, is $\varepsilon_k N_k$ where N_k is the number of particles in the k^{th} state. Thus the Boltzmannn factor of the k^{th} state of the system is just $\left[e^{\beta(\mu-\varepsilon_k)}\right]^{N_k}$. Here, $\beta = 1/k_B T$, μ is the chemical potential and $\varepsilon_k = \varepsilon_k(S, V, N_k)$ is related to the entropic and extensive energy $E_K(S, V) = \varepsilon_k(S, V, N_k) \times N_k$ of the k^{th} state . The limitless supply of particles ensures that the k states are independent, thus we know that the grand partition function for a configuration of our system involving $\{N_1, \ldots, N_k, \ldots\}$ particle sets is the product of

the individual Boltzmannn factors

$$\begin{aligned}\mathcal{Z}_{configuration} &= \left[e^{\beta(\mu-\varepsilon_1)}\right]^{N_1}\cdots\left[e^{\beta(\mu-\varepsilon_k)}\right]^{N_k}\cdots \\ &= \prod_k e^{\beta(\mu-\varepsilon_k)N_k}\end{aligned} \tag{2}$$

We attempt to use this in a classical setting. Consider our familiar classical particles. In general it seems that any one of them can have any energy at all so long as the energy is available. Recall that we are interested in occupation numbers, that is, the allowed number of particles in a given state, since Pauli's exclusion principle proves so fruitful. For classical particles then it seems the occupation number n_k of the k^{th} energy state is unrestricted so long as the particle number N_k is unrestricted. So the classical occupation numbers are $\{n_k\} = \{\{0,1,\ldots\},\{0,1,\ldots\},\ldots\}$.

Because a partition function acts as a normalization factor for a system it must account for all possible configurations of a system; for a grand canonical ensemble with varying particle number, to consider all possible particle numbers $\{N_k\}$ is just to consider all allowed particle numbers n_k. Let us try this for the classical case.

$$\begin{aligned}\mathcal{Z} &= \sum_{n_k=0}^{\infty}\prod_k e^{\beta(\mu-\varepsilon_k)n_k} \\ &= \prod_k\sum_{n_k=0}^{\infty} e^{\beta(\mu-\varepsilon_k)n_k} \\ &= \prod_k\left(1+e^{\beta(\mu-\varepsilon_1)}+e^{2\beta(\mu-\varepsilon_2)}+\ldots\right) \\ &= \prod_k\frac{1}{1-e^{\beta(\mu-\varepsilon_k)}}\end{aligned} \tag{3}$$

The infinite sum and thus the independence of k and n_k allow us to factor out the product over states.[4] From Equation 3 we can derive numerous things; of interest is the average number of particles per state, which we call the filling factor.

$$\langle n_k\rangle = \frac{1}{\beta}\frac{\partial\log\mathcal{Z}_k}{\partial\mu} \tag{4}$$

where

$$\log\mathcal{Z} = \sum_k\log\left(\frac{1}{1-e^{\beta(\mu-\varepsilon_k)}}\right) = \sum_k\log\mathcal{Z}_k$$

Thus we have for our filling factor

$$\begin{aligned}\langle n_k\rangle &= -\frac{1}{\beta}\frac{\partial}{\partial\mu}\log(1-e^{\beta(\mu-\varepsilon_k)}) \\ &= \frac{1}{e^{\beta(\varepsilon_k-\mu)}-1}\end{aligned} \tag{5}$$

This is surprising. We used what we thought were classical occupation numbers so it is reasonable to expect a classical result. However, classical physics tells us that a particle has the probability $e^{-\beta\varepsilon_k}$ to occupy a state of energy ε_k, thus classically we expect the mean number of particles occupying a state of energy ε_k to be proportional to $e^{-\beta\varepsilon_k}$ modified by a chemical potential $e^{\beta\mu}$ if it is a grand canonical ensemble. $\langle n_k\rangle$ for a classical system ought to be $\langle n_k\rangle = e^{-\beta(\varepsilon_k-\mu)}$.

Furthermore, compare our result to Planck's blackbody distribution.

$$\langle n_k\rangle = \frac{1}{e^{\beta(\varepsilon_k-\mu)}-1} \qquad u(\omega) = \frac{\omega^2}{\pi^2c^3}\;\frac{\hbar\omega}{e^{-\beta\hbar\omega}-1}$$

So if $\mu = 0$ in Equation 5, this factor appears in the blackbody distribtuion: $u(\omega)$ is the energy density due to photons, and given that photons have energy $E_k = \hbar|k|/c = \hbar\omega$ we have $u(\omega) = E_k\langle n_k\rangle$. The number of photons in the universe is not conserved so we can justify setting $\mu = 0$. The factor $\frac{\omega^2}{\pi^2c^3}$ is related to the degeneracy of the energy state. We derived not the classical distribution we expected, but a quantum mechanical one. It is reasonable to suspect that the classical occupation numbers are also those for bosons; we consider further evidence below in Section V.

IV. FILLING FACTORS

We have discovered that classical states and bosonic quantum states share the same set of allowed occupation numbers, though their filling factors differ. Thus it seems the difference between classical and quantum behaviour lies either in the particles themselves or in another property of the states we have yet to discover.

Let us turn our attention now to the particles. For the moment we know nothing of individual particles; our equations only concern congregations of particles. Having obtained the allowed occupation numbers it is useful to consider a microcanonical ensemble for which the total particle number is fixed. Given a particular configuration of particles we can factor a microcanonical ensemble of total energy E into a smaller microcanonical ensemble of energy E_k. Consider a particular macrostate of energy E_k which has g_k microstates.[5] In other words, the k^{th} state has energy E_k with degeneracy g_k. Now imagine N_k particles of our total number $N = \sum_k N_k$ live in the k^{th} energy state. Evidently there is ample room since each of the g_k degenerate states have unlimited capacity given our infinite sets of classical and bosonic occupation numbers.

Consider the k^{th} state. We know of two ways to distribute the N_k particles over the g_k microstates. If we distinguish between the N_k particles, the number of distinct arrangements over g_k states is just

$$(g_k)^{N_k}$$

On the other hand if we do not distinguish between them, the number of distinct arrangements is

$$\frac{(N_k + g_k - 1)!}{(N_k)!(g_k - 1)!}$$

Whether or not we distinguish between our particles has ramifications for our full system.[6] If we've partitioned our system into R microstates of energies $E_1, E_2, \ldots, E_R$, then the number of distinct arrangements of the $N_1, N_2, \ldots, N_R$ sets of distinguished particles over the R energy levels is $(N!)/(N_1! \ldots N_R!)$ so the total number of arrangements is

$$\begin{aligned} W_D &= \sum_{\{N_k\}} \frac{N!}{N_1! \ldots N_R!} \prod_{k=1}^{R} (g_k)^{N_k} \\ &= \sum_{\{N_k\}} N! \prod_{k=1}^{R} \frac{(g_k)^{N_k}}{N_k!} \end{aligned} \tag{6}$$

For any set $\{N_k\}$ of undistinguished particles, there is only one arrangement of N particles over R energy states, so the total number of arrangements is

$$W_U = \sum_{\{N_k\}} \prod_{k=1}^{R} \frac{(N_k + g_k - 1)!}{(N_k)!(g_k - 1)!} \tag{7}$$

We've yet to associate these combinatorial accounts with anything, but using Boltzmann's statistical definition of entropy $S = k_b \log W$ as our launchpad, let's see what we can make of them. We use Sterling's formula $\log(N!) \approx N \log N - N$. Then for a particular set $\{N_k\}$,

$$\begin{aligned} S_D &= k_B \log W_D \\ &= k_B \log\left(N! \prod_{k=1}^{R} \frac{(g_k)^{N_k}}{N_k!} \right) \\ &= k_B (N \log N - N) + \\ &\qquad + \sum_{k}^{R} (N_k \log g_k - N_k \log N_k + N_k) \end{aligned} \tag{8}$$

Recall that a system in equilibrium maximizes its entropy. Let us do so, with the constraints that $N = \sum_k^R N_k$ and $E = \sum_k^R N_k E_k$ are constant. We use the method of Lagrange variables and require $\nabla(S - \alpha N - \beta E) = 0$ where α, β are arbitrary constants. Evidently

$$\begin{aligned} \frac{\partial}{\partial N_k}(S - \alpha N - \beta E) &= \frac{\partial}{\partial N_k}\Big(k_B \Big[\log(N!) + \sum_{k}^{R} (N_k \log g_k - N_k \log N_k + N_k) \Big] \\ &\qquad - \alpha \sum_{j}^{R} N_j - \beta \sum_{i}^{R} N_i E_i \Big) \\ &= k_b \sum_{k}^{R} \log\Big(\frac{g_k}{N_k}\Big) - \alpha - \beta E_k \\ &= 0 \end{aligned} \tag{9}$$

Notice that $\left(\frac{N_k}{g_k}\right)$ is the mean occupation number, our filling factor $\langle n_k \rangle$, so at equilibrium our system of distinguished particles has

$$\langle n_k \rangle = \frac{1}{e^{\alpha + \beta E_k}} \tag{10}$$

This is just the form given by classical statistical mechanics. What of our system of undistinguished parti-

$$\begin{aligned} S_U &= k_B \log W_U \\ &= k_B \log\Big(\prod_{k=1}^{R} \frac{(N_k+g_k-1)!}{(N_k)!(g_k-1)!}\Big) \\ &= k_B \sum_{k=1}^{R} \log\Big(\frac{(N_k+g_k-1)!}{(N_k)!(g_k-1)!}\Big) \\ &= k_B \sum_{k=1}^{R} \log\Big(\frac{g_k}{N_k+g_k}\Big) + \log\Big(\frac{(N_k+g_k)!}{(N_k)!(g_k)!}\Big) \\ &= k_B \sum_{k=1}^{R} (N_k+g_k)\log(N_k+g_k) - N_k \log N_K - g_k \log g_k \end{aligned} \tag{11}$$

As above we maximize the entropy,

$$\begin{aligned} \frac{\partial}{\partial N_k}(S-\alpha N-\beta E) = \frac{\partial}{\partial N_k}\Big(k_B \sum_{k=1}^{R}[(N_k+g_k)\log(N_k+g_k) - N_k \log N_K - g_k \log g_k] \\ - \alpha \sum_{j}^{R} N_j - \beta \sum_{i}^{R} N_i E_i\Big) \\ = k_b \sum_{k}^{R} \log\Big(\frac{g_k}{N_k}\Big) - \alpha - \beta E_k \\ = 0 \end{aligned} \tag{12}$$

We solve this to obtain

$$\langle n_k \rangle = \frac{1}{e^{\alpha+\beta E_k}-1} \tag{13}$$

This is precisely of the form of the bosonic filling factor! Our microcanonical ensemble seems to tell us that we distinguish between classical particles, but we do not distinguish between bosons. A similar exercise tells us that fermions are likewise undistinguished.[7]

Before we adopt this distinction between classical and quantum particles as authoritative, it would behoove us to confirm that we can reproduce the classical result in a more general setting.

V. PARTICLES

Our discussion of the microcanonical ensemble provides a clue to how we achieved quantum statistics from a classical proposition. In our haphazard construction of the grand partition function above, the only decisive decision was to consider an unrestricted occupation number. This is precisely what classical particles and bosons share. This leads us to believe that somewhere in our partition function we must have included the fact that our particles were indistinguishable. It is not obvious where. Our formulation above worked more with the states the particles occupy than the particles themselves. Can we build our system from the particles, thereby imposing whether or not we distinguish between them? Following, we adopt the working definitions of classical particles as those which give classical statistics, and quantum particles as those which give quantum statistics

Consider a canonical ensemble of noninteracting particles. The form of its partition function allows us to factor it into single-particle states. Thus, discussion of a single-particle is entirely sensible when working with canonical ensembles. Indeed it is often the case that we reverse the logic and use the single-particle partition function to build the entire system's.

It is tempting to take this same approach for our grand canonical ensemble, in which our primary interests lie. The astute reader realizes that while single-particle partition functions are natural in canonical ensembles, we must not forget that for grand canonical ensembles the chemical potential is a parameter of the system: $dE = TdS - pdV - \mu dN$. For systems of few particles, dN is a nonsensical expression, the continuum limit absurd. This is true but trivial if we use the partial trace.

Nothing stops us from separating the energy into its independent contributions "$TdS - pdV$" and "μdN." We

follow convention and write "$dE = TdS - pdV$," so the total energy is "$dE + \mu dN$." Separating these terms allows us to disentangle the two degrees of freedom of our ensemble: "μdN" corresponds to the exchange of particles between system and reservoir along with all the energy due to this exchange, and "dE" corresponds to the remaining free energy.[8] This energy is just that which a canonical ensemble exchanges with the reservoir. Nothing stops us from first considering the behaviour of the system associated with "dE," then that associated with "μdN." Equivalently, nothing stops us from considering the primitives of the grand canonical ensemble to be canonical ensembles. So with nothing stopping us, let us start.

The partition function for a single particle is just

$$Z_1 = \sum_k e^{-\beta E_k} \tag{14}$$

where $E_k = E_k(S, V)$ is of the canonical variety of energy. Let us consider N such particles, noninteracting and distinguishable.

$$\begin{aligned} Z_N &= \sum_{k_1,\ldots,k_N} e^{-\beta(E_{k_1}+\ldots+E_{k_N})} \\ &= \prod_{j=1}^{N}\Big(\sum_{k_j} e^{-\beta E_{k_j}}\Big) \\ &= \Big(\sum_k e^{-\beta E_k}\Big)^N \\ &= \Big(Z_1\Big)^N \end{aligned} \tag{15}$$

where the last two equalities follow from the particles' identical energy spectra. Realize that we do not insist that each energy E_k is a function of N, for the power is taken over the entire sum, not a particular Boltzmann factor. Indeed we may not do so for we insist that we work with particles, not with energy states or their occupation numbers.

Now we make our canonical ensemble grand. Evidently we must sum over all possible particle numbers and account for the energy due to each.

$$\begin{aligned} \mathcal{Z} &= \sum_{N=0}^{\infty}\Big(Z_1\Big)^N e^{\beta\mu N} \\ &= \sum_{N=0}^{\infty}\Big(\sum_k e^{-\beta(E_k-\mu)}\Big)^N \\ &= \frac{1}{\Big(1-\sum_k e^{-\beta(E_k-\mu)}\Big)} \end{aligned} \tag{16}$$

We are primarily concerned with the derivatives of the logarithm for it is these that determine the physical properties of our system.

$$\log \mathcal{Z} = -\log\Big(1 - \sum_k e^{-\beta(E_k-\mu)}\Big) \tag{17}$$

This expression diverges quickly to infinity, so any derivative is undefined. It seems we've recovered the ultraviolet catastrophe.

Although we did not get the classical Boltzmann filling factor from distinguished particles, we did arrive at our classical prediction. This is somewhat encouraging, so let us see if we can recover quantum predictions building explicitly from a system of undistinguished particles. The single-particle partition function Equation 14 is the same in either case. But for undistinguished particles the summation Equation 15 over all particle states includes energy states which differ only by permutations of the particles and are thus the same for undistinguished particles. These must be identified. Such a task calls for combinatorics, but a more mundane approach proves illuminating.

Starting with a simple case, suppose our system consists of particles all in different energy states. Then there are $N!$ ways to arrange our N particles throughout the states, so identifying all the permutations amounts to dividing our partition function for N distinguishable particles by $N!$,

$$Z_N = \frac{1}{N!} Z_1^N$$

which gives a grand partition function

$$\begin{aligned} \mathcal{Z}_N &= \sum_N \frac{1}{N!} Z_1^N e^{\beta\mu N} \\ &= \sum_N \frac{1}{N!}\Big(\sum_k e^{-\beta(E_k-\mu)}\Big)^N \\ &= \exp\Big(\sum_k e^{-\beta(E_k-\mu)}\Big) \\ &= \prod_k \exp\Big(e^{-\beta(E_k-\mu)}\Big) \end{aligned} \tag{18}$$

giving us

$$\begin{aligned} \log \mathcal{Z}_N &= \sum_k e^{-\beta(E_k-\mu)} \\ &= \sum_k \log \mathcal{Z}_k \end{aligned} \tag{19}$$

and

$$\begin{aligned} \langle n_k \rangle &= \frac{1}{\beta}\frac{\partial}{\partial\mu}\log \mathcal{Z}_k \\ &= e^{-\beta(E_k-\mu)} \end{aligned} \tag{20}$$

But this is the Boltzmann factor, which we expect for classical particles, which our microcanonical ensemble via Equation 10 suggests is composed of distinguished particles.

Our formulation of the system involved the key assumption that we do not distinguish between the particles. In the first case we considered, we derived quantum statistics from classical occupation numbers. We resolved

this by supposing we had not correctly accounted for the distinguishibility of the particles. In our most recent case we derived classical statistics from a system of undistinguished particles. We must try to extract ourselves from this muddle of classical and quantum conditions and results. Clearly we can no longer say with confidence: "classical particles are distinguishable, quantum particles are not." A reasonable solution to our conundrum is to concede that all particles, classical and quantum, may be undistinguished, and to attribute the diverging behaviour of undistinguished classical and quantum particle statistics to a different reason, uniquely quantum. We discuss the reasons for and the consequences of this solution in the accompanying paper, for which I am thankful to my advisor Professor Katherine Brading for many enlightening discussions and wonderful insights.

[1]W. Pauli, *Exclusion principle and quantum mechanics* (Éds. du Griffon, 1947).
[2]K.M. Blundell, *Concepts in thermal physics* (Oxford University Press, USA, 2006).
[3]J.P. Sethna, *Statistical mechanics: entropy, order parameters, and complexity* (Oxford University Press, USA, 2006).
[4]We will discuss the ramifications of the assumption involved for this step in detail in our accompanying paper upon mentioning it below in Section V. In short, in writing this equality we do not carefully consider how the identification of N_k with n_k affects the energy ε_k. Thank you to Professor Antonio Delgado for requiring a rigorous explanation for this equality.
[5]The terminology here is cumbersome. Microcanonical ensembles have fixed energies; here each smaller macrocanonical ensemble is a macrostate of energy E_k. Our macrostate has observable properties. It contains a certain number of unobservable microstates, each equally likely to be occupied. Thus probability of a particular macrostate is directly proportional to the number of microstates it contains.
[6]SJ Bence, KF Riley, and MP Hobson, *Mathematical Methods for Physics and Engineering: A Comprehensive Guide* (Cambridge: Cambridge University Press, 2006).
[7]Thank you to Professor S. Blundell for suggesting this as an exercise.
[8]There is a subtle but important difference between the situation at hand and that considered in Equation 3. Here we have a variable $E(S,V)$ independent of the particle number N. If we were to relate $E_k = E_k(S_k, V)$ to the particle number N_k via $E_k = \varepsilon_k N_k$, we would have to vary ε_k in conjunction with N_k. For the case of Equation 3, if we were so inclined to equate the occupation number with the particle number, we would be forced to vary E_k upon varying the particle number for it is ε_k that is constant. Thus we see we had already built into our partition function quantum mechanical packets of discrete energy. We will explore the significance of this in detail in the accompanying paper.

Determination of Neutron Branching in the ^{12}C +^{12}C Fusion Reaction

Justin Browne
University of Notre Dame, Department of Physics

Abstract

The neutron branch of the ^{12}C+^{12}C fusion reaction is important for the carbon shell burning and carbon explosive burning. The ^{23}Mg created by the ^{12}C(^{12}C,n)^{23}Mg reaction may undergo β^+ decay, changing the neutron excess in the combusting material inside of metal-poor stars, and the neutrons emitted from this reaction may contribute to the weak s-process. To measure the branching ratio of the neutron emission channel of the ^{12}C+^{12}C fusion reaction, a detection system, consisting of an array of four plastic scintillators and two Germanium detectors, has been developed to detect the decay of the ^{23}Mg. The system have been tested at $E_{c.m.}$ =4.24 MeV. Using $\beta^+ - \gamma$ coincidence technique, the ^{23}Mg reaction products has been unambiguously identified.

1 Introduction

The ^{12}C(^{12}C,n)^{23}Mg reaction is important for two reasons: the ^{23}Mg can undergo β^+ decay, changing the overall neutron to proton ratio, and a neutron is emitted from the nucleus.

^{23}Mg undergoes β^+ decay. In β^+ decay, a proton is changed into a neutron, positron, and electron neutrino. In the early universe, Hydrogen made up about 75% of the mass and Helium made up about 25%. This means there was about a 1:7 neutron to proton ratio. Today, that ratio is much higher. There are many more heavy elements that have more neutrons that protons in their nuclei. ^{23}Mg decay is one of the major processes that turns protons into neutrons [1].

The ^{12}C(^{12}C,n)^{23}Mg reaction produces free neutrons, which can be used in the s-process. The s-process, or slow neutron capture process, involves a nucleus capturing neutrons until it becomes unstable. Then, the nucleus

β^- decays until it becomes stable. The nucleus works its way up the valley of stability by capturing neutrons and β^- decaying. By knowing the rate at which ^{12}C(^{12}C,n)^{23}Mg occurs, we can predict the abundance of heavy elements in stars and compare it to abundances in real stars.

We hope to determine the branching ratio of the neutron channel (β_n). To determine this, we will need to find the cross section (σ). The branching ratio is the ratio of the cross section of the reaction you are interested it divided by the sum of the cross sections of all reactiions and is defined by

$$\beta_n \equiv \frac{\sigma_n}{\sigma_n + \sigma_p + \sigma_\alpha}. \quad (1)$$

The cross section is the probability that a reaction will occur. In a thick target, which we are using, the cross section can be determined using the equation

$$\sigma = \frac{M_T}{f N_A} \frac{dY}{dE} \frac{dE}{d(\rho x)}, \quad (2)$$

where M_T is the molecular weight, f is the molecular fraction, N_A is Avogadro's Number, dY/dE is the differential yield (how much the yield changes when you change energy), and $dE/d(\rho x)$ is the stopping power of the target [2]. To find the branching ratio and cross section of this reaction, we need to find the yield at multiple energies.

2 Experimental Setup

In the laboratory, we simulate this process by bombarding the ^{12}C target with an intense ^{12}C beam. The neutron production yield can be determined by detecting the β^+ decay of 23Mg, which will help us understand the rate at which this reaction occurs in stars. The way we do this is by detecting γ-rays with a Germanium detector and detecting β^+-particles with a scintillator detector.

When ^{23}Mg decays, it emits a β^+-particle. A β^+-particle is a positron, the anti-matter counterpart to an electron. When an electron and a positron collide, they annihilate, changing into pure energy, light. In order to conserve momentum, two photons (or γ-rays) must be created, each one having the energy equivalent to the mass of a positron and electron, 511 keV. When we detect a β^+-particle and a 511 keV γ-ray at the same time, we claim that it is from ^{23}Mg decay.

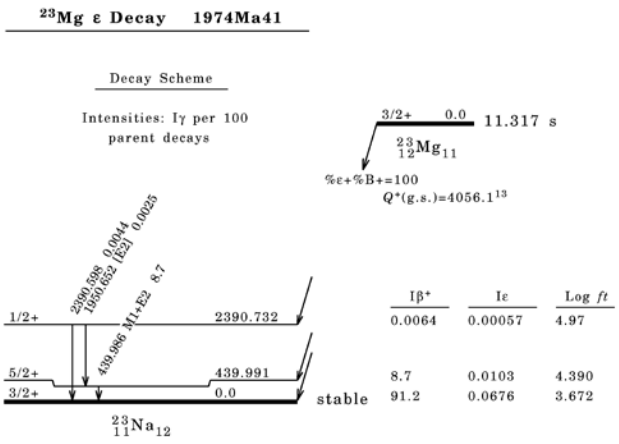


Figure 1: The decay scheme for ^{23}Mg [3].

Fig. 1 shows the decay scheme for ^{23}Mg. From this decay scheme, we see that 91.2% of the time ^{23}Mg β^+ decays to ^{23}Na in the ground state and 8.7% of the time ^{23}Mg β^+ decays to ^{23}Na in the ground state and emits a 440 keV γ-ray.

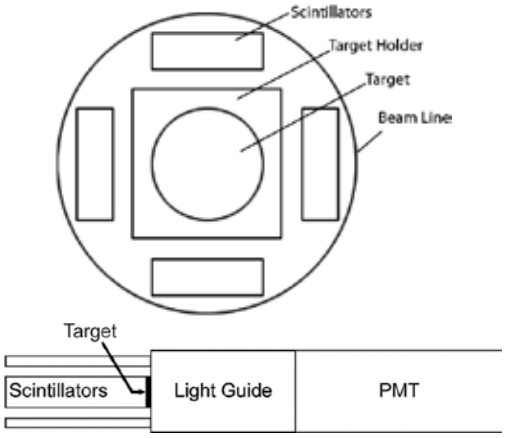


Figure 2: Front (above) and side (below) views of the scintillator array.

The detector we used to detect β^+-particles was an array of four plastic scintillators arranged as in Fig. 2. The scintillators are blocks of special plastic that emit light when a particle passes through them; the color of the light depends upon the energy of the incident particle. After cutting the plastic, we sanded and polished them to provide a smooth surface to improve light transmission. The scintillators were placed upstream of the target, and were glued to a Lucite light guide right behind the target, and the light guide was coupled to a photomultiplier tube (PMT). A PMT takes a small amount of light and amplifies it, so that we can record it more easily. We noticed that the detector was sensitive to protons and α-particles, so we wrapped the scintillators in aluminized mylar foil because β-particles are able to penetrate the foil, but the background protons and α-particles cannot. We used two Germanium detectors to detect γ-rays. Though we had two Ge detectors, we only used one of them during the data analysis because the other had very poor resolution.

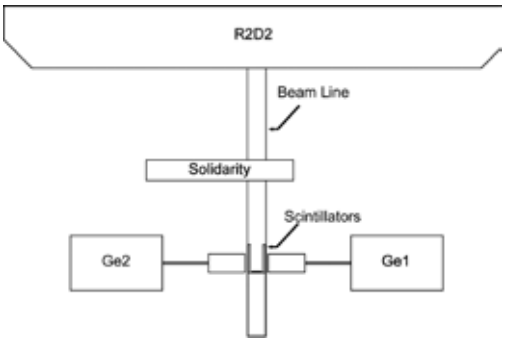


Figure 3: Diagram of the experimental setup, as seen from above

We want to find out how much ^{23}Mg is produced during our experiment, so we decided to measure the decay of ^{23}Mg, which has a half-life of 11.317 s. To do this, we irradiated our ^{12}C target for 20 s, and blocked the beam for 40 s (about 2 and 4 half-lives, respectively), so that we could measure the ^{23}Mg decay without any more being produced. We used SOLIDARITY, a rotating wheel system, to rotate between a collimator and a piece of Aluminum. The beam irradiated the target when the collimator is in position. The decay measurement was performed while the Aluminum was in place to block the beam. Fig. 3 shows a diagram of our experimental setup.

3 Measurements and Analysis

A series of measurements were taken at the center of mass energy of 4.24 MeV, an energy that was high enough to give us clear

results. Fig. 4 shows the γ-ray spectrum obtained from the Ge detectors. Interesting peaks include the 440 and 511 keV peaks. The 440 peak, barely above background in the ungated spectrum, is enhanced through $\beta - \gamma$ coincidence, and is about 9% the size of the 511 peak, in agreement with the decay scheme (Fig. 1).

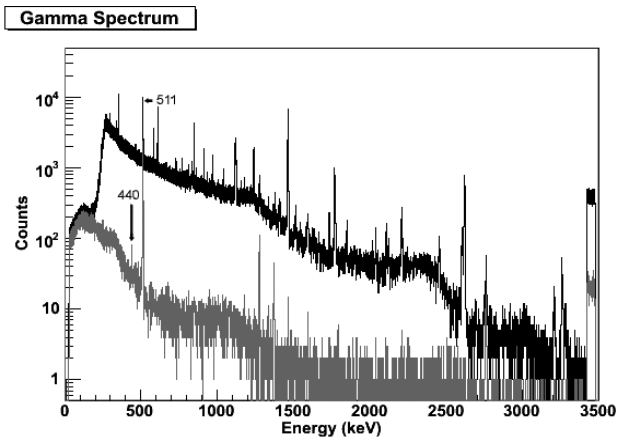


Figure 4: The raw γ-ray spectrum (dark) and the γ-ray spectrum gated by β-particles (light).

Since we claim that when we detect a 511 keV γ-ray and a β-particle at the same time, we are witnessing ^{23}Mg decay, we need to confirm this. We could compare different sections, which are shown in Fig. 5. The different sections should have the following number of counts as described in Eq. 3, where N is the initial activity, λ is the decay constant (which is 0.06125 s^{-1} for ^{23}Mg), and K is the background contribution including long lived reaction products and the natural background. Using the exponential decay law (Eq. 3), we can derive Eq. 4, where R is a ratio that is convenient for comparing the

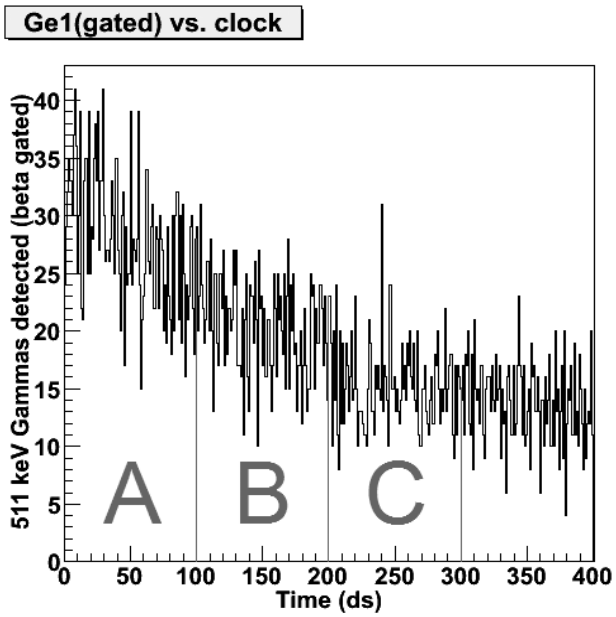


Figure 5: The number of 511 γ-rays detected with respect to time, split into three 10 s intervals.

experimental and theoretical decay constant.

$$\begin{aligned} A &= N(1 - e^{-\lambda 10}) + K \\ B &= N(e^{-\lambda 10} - e^{-\lambda 20}) + K \\ C &= N(e^{-\lambda 20} - e^{-\lambda 30}) + K \end{aligned} \tag{3}$$

$$R = \frac{A - C}{B - C} \tag{4}$$

We can now compare the experimental value of R to the theoretical value. Experimentally, we calculated $R = 2.42 \pm 0.31$, and theoretically, $R = 2.85$. This is close, but it suggests that there might be some other activity represented in our data.

Another way to confirm that we are detecting ^{23}Mg is by fitting a curve to the decay. By doing so we can not only see if the

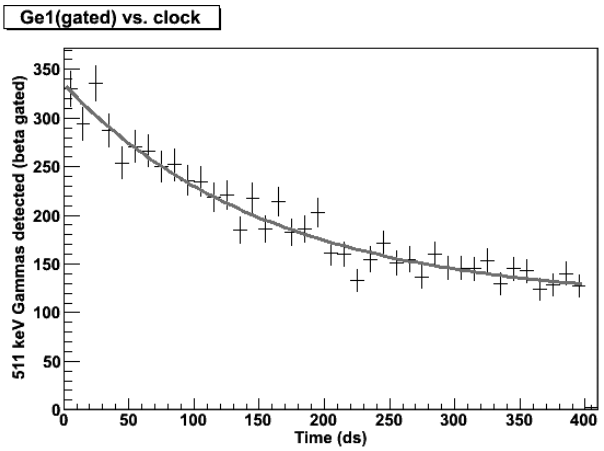


Figure 6: The number of 511 γ-rays detected with respect to time, with an exponential decay curve fit to it.

λ we determine from our measurements corresponds to the λ of ^{23}Mg but we can also extrapolate the curve to find how much ^{23}Mg we produce. The fit curve can be seen in Fig. 6, and is of the form $N(t) = N_0 e^{-\lambda t} + K$. The decay constant, λ, was calculated to be $\lambda = 0.0635 \pm 0.0087\ \mathrm{s}^{-1}$, which is within error of the accepted value, $\lambda = 0.06125\ \mathrm{s}^{-1}$. Using this fit, we can find an approximate value for how much ^{23}Mg we produced. We can integrate from when the beam was blocked (t_0) to infinity, and divide by the detector efficiencies, as in Eq. 5:

$$Y = \int_{t_0}^{\infty} N(t)dt/\varepsilon_\gamma\varepsilon_\beta, \tag{5}$$

where $N(t) = N_0 e^{-\lambda t}$, ε_γ is the efficiency of the Germanium detector, and ε_β is the efficiency of the β detector.

To determine the absolute yield (from Eq. 5) of the produced ^{23}Mg we need to know the detector efficiencies. To determine the efficiencies, we use the coincidence method. The number of 511 keV γ-rays we detect is described by Eq. 6, and the number of 511 keV γ-rays we detect at the same as a β-particle is described by Eq. 7.

$$N_u = N\varepsilon_\gamma \tag{6}$$
$$N_g = N\varepsilon_\gamma\varepsilon_\beta \tag{7}$$

From Eq. 6 and 7, we can derive the beta efficiency:

$$\varepsilon_\beta = \frac{N_g}{N_u} \tag{8}$$

However, to get N_g and N_u, we need to subtract the background. We can use the last 10 s of our decay as the background, since only contains 6.25% of the total decays. We will use $T1_u$, $T4_u$, $T1_g$, and $T4_g$ as the integral of 511 keV peak during the first 10 s ungated, last 10 s ungated, first 10 s gated, and last 10 s gated, respectively.

$$\begin{aligned} T1_u &= N\varepsilon_\gamma(1 - e^{-\lambda 10}) + K \\ T4_u &= N\varepsilon_\gamma(e^{-\lambda 30} - e^{-\lambda 40}) + K \\ T1_g &= N\varepsilon_\gamma\varepsilon_\beta(1 - e^{-\lambda 10}) + K \\ T4_g &= N\varepsilon_\gamma\varepsilon_\beta(e^{-\lambda 30} - e^{-\lambda 40}) + K \\ \varepsilon_\beta &= \frac{T1_g - T4_g}{T1_u - T4_u} \end{aligned} \tag{9}$$

Similarly, we can use the β spectrum, gated and ungated by a 511 keV γ-ray, to determine the γ efficiency.

Using the background subtraction coincidence method described above we see the 511 keV peaks and the β spectrum shown in Fig. 7. The efficiencies obtained by this method were $\varepsilon_\beta = 62.0 \pm 4.7\%$ and $\varepsilon_\gamma = 2.43 \pm 0.12\%$. These efficiencies seem to be

too high, especially ε_β because the detector only covers ∼25% solid angle. We have developed some theories for why the efficiencies were so high. One is that the β-particles could be bouncing off of the ^{12}C target, deflecting back towards the detector. Also, the 511 keV γ-rays are emitted from the positron, not the target, so a 511 keV γ-ray emitted from a detected positron is more likely to be detected than one emitted from an undetected positron because of the geometry.

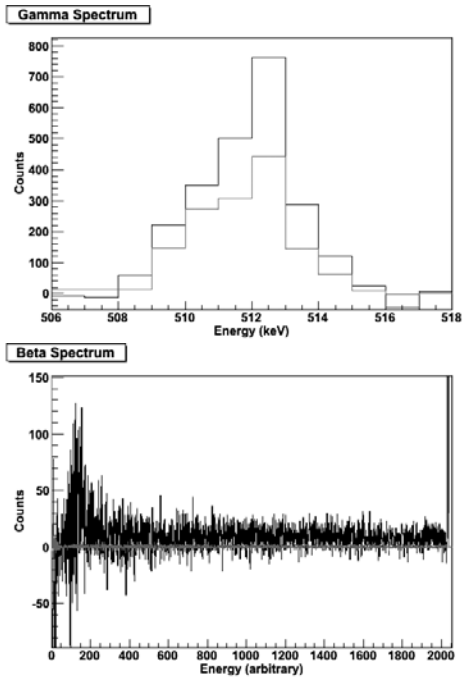


Figure 7: The 511 peak ungated (top, dark) and gated (top,light) with background subtracted. The ungated (bottom, dark) and gated (bottom, light) β spectra with background subtraction.

Using these efficiencies and Eq. 5, we can determine the absolute yield. The value we obtained was $Y = (2.39 \pm 0.40) \times 10^6$. To normalize the data, we divided by the number of incident ^{12}C, and the resulting normalized yield was $Y_n = (1.30 \pm 0.22) \times 10^{-10}$.

4 Discussion and Conclusions

L. Barrón-Palos et al. conducted a similar experiment in which they measured the proton, alpha, and neutron channels [2]. We plan to push measurements of the neutron channel further than that experiment, but their data will provide a good comparison as we collect more data points. This measured thick target yield is based on the online γ-rays. Therefore, all the transition to the ground states of the final products are excluded from the final result. The yield from the decay measurement should be higher because it includes both transitions to the first excited state and the final state. The yield we obtained was about an order of magnitude higher than their prediction (about 1.1×10^{-11}). This ratio may be too high to be real. It might indicate there are some problems with the detector efficiencies. For example, the efficiency of the beta counter is even larger than its geometric efficiency (∼25%). It may be because the 5 mm thick plastic detector is sensitive to the γ-rays. The γ-ray detection efficiency should be checked with a standard source as well. To determine the cross section and branching ratio, we need to know the differential yield (dY/dE), so the yield must be measured at more energies before any definite conclusions can be made.

This experiment showed that our setup is capable of detecting trace amount of ^{23}Mg from the ^{12}C+^{12}C fusion reaction, and we can continue these measurements at more energies. For the future experiments, we want to make a new scintillator setup. The new setup will make use of small PMTs that can fit inside the beamline. Using these small PMTs will free up the area directly behind the target, so we can put a Germanium detector there, covering approximately 2π solid angle and increasing the overall efficiency of our detection system. The new set up will resemble Fig. 8.

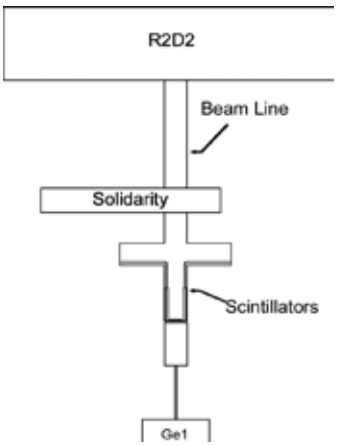


Figure 8: A diagram of the future experimental setup.

Acknowledgements

I would like to thank Dr. Xiaodong Tang for his wonderful guidance. I would also like to thank everyone in my research group, Masahiro Notani, Ali Snedden, Brian Bucher, Spencer Thomas, Chi Ma, Xiao Fang, and Camille Garcia. I would also like to show my appreciation to Dr. Garg and Ms. Herman for organizing and helping, in many ways, us with our summer research. This research was supported in part by the National Science Foundation under Grant Numbers NSF-PHY05-52843 and PHY07-58100.

References

[1] Arnett, D., *Supernovae and Nucleosynthesis*, 1996, Princeton University Press.

[2] L. Barrón-Palos et al., *Nuclear Physics A 779* (2006) 318332.

[3] Data extracted using the NNDC On-Line Data Service from the ENSDF database, file revised as of Aug 27, 2009. M.R.Bhat, Evaluated Nuclear Structure Data File (ENSDF), R.B. Firestone, "Nuclear Data Sheets for A = 23", *Nuclear Data Sheets*, Volume 108, Issue 1, January 2007, Pages 1-78, ISSN 0090-3752, DOI: 10.1016/j.nds.2007.01.002.

Visit

Read past articles, browse new ones, and submit your own research online at http://scientia.nd.edu.

For more information about undergraduate research at the University of Notre Dame, visit http://science.nd.edu/undergradresearch.

Contact

Email questions or comments to the editors at scientia@nd.edu.

Join

Get involved with Scientia as an editor, news columnist, or graphic designer for the upcoming semester.
Email for details.