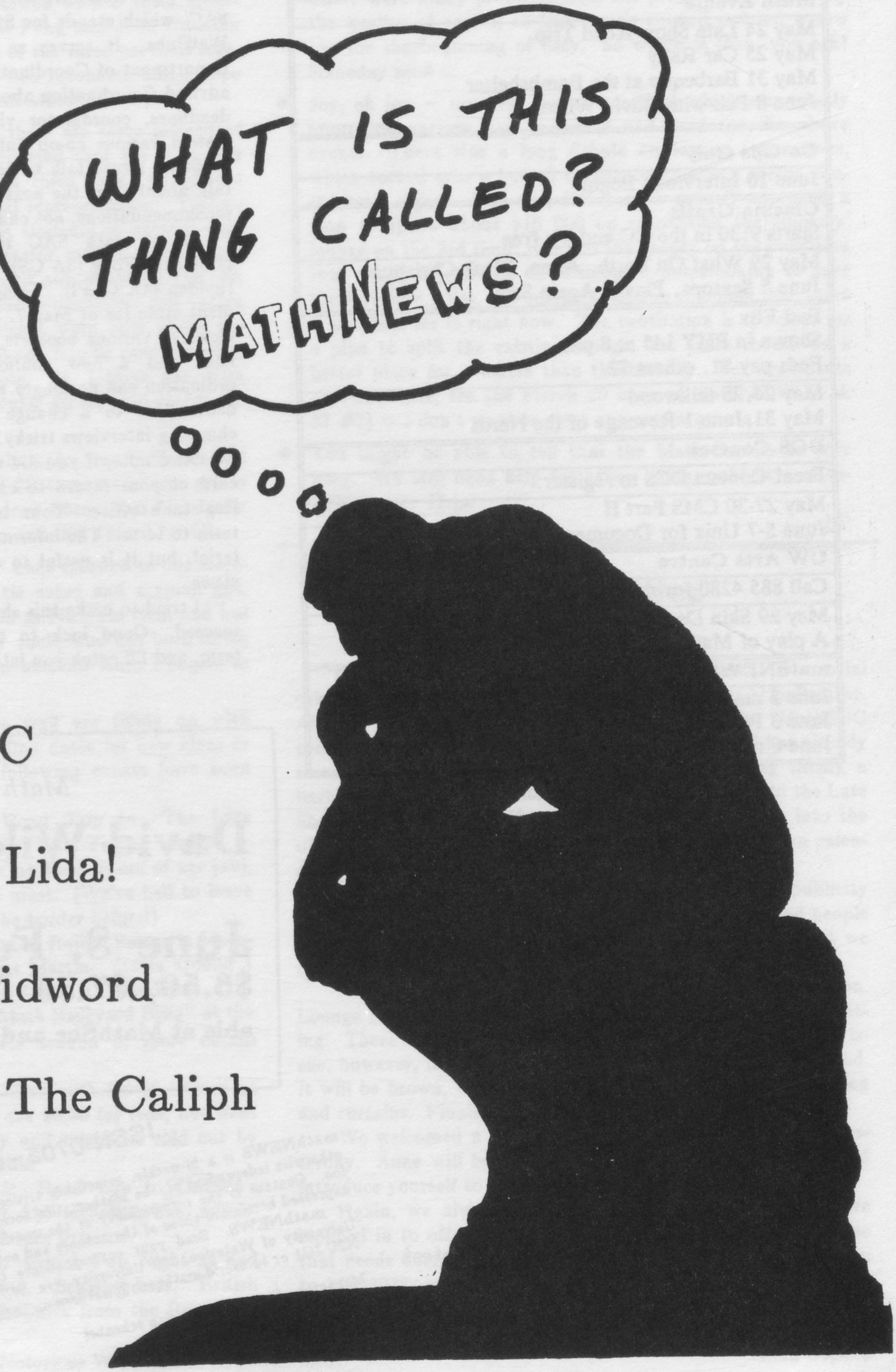
MATHNEWS

Volume 38
Number Two

Fridae May 24



LookAhead

A glance at upcoming events

Math Events

May 24 Late Show Road Trip
May 25 Car Rally
May 31 Barbeque at the Bombshelter
June 8 Pub with David Wilcox

Co-Ops Only

June 10 Interviews Begin

Cinema Gratis

Starts 9:30 in the CC and it's free

May 29 What On Earth, Alien, Black Christmas
June 5 Seasons, Play It Again Sam

Fed Flix

Shown in PHY 145 at 8 pm.
Feds pay $1, others $2

May 24,25 Silkwood
May 31,June 1 Revenge of the Nerds

DCS Courses

Free! Contact DCS to register.

May 27-30 CMS Part II
June 5-7 Unix for Documentation

UW Arts Centre

Call 885 4280 for more info and tickets

May 29 Skin Deep
A play of Martin Luther King

mathNEWS Important Dates

June 2 mathNEWS Articles Deadline
June 3 Production Night
June 8 next mathNEWS hits the streets

Tired of the Old Math T-Shirts?
Design a New One!

Address Entries to Jane in
MathSoc (MC 3038) by
4:30 June 6th

Winner Gets the First
T-Shirt Plus
2 Tickets to:
David Wilcox
British Pub Night
The Wine & Cheese
End-of-Term Pub

Contest Contest Contest Contest

Cul-de-SAC

Last week's article was not meant to be titled "In the SAC", but that's what I get when I leave articles untitled! The SAC, which stands for Student Advisory Council, does not run WatPubs. It serves as a liaison between students and the Department of Coordination and Placement. In the past it has advised Coordination about student views on policies, want ads, deadlines, coordinator visits, and work reports, and has reviewed various co-op publications. If you have a question or problem, please talk to one of the math reps and we will try to talk about it at the next meeting (although we can only make recommendations, not changes).

Your math SAC reps are Brett Martin (2B ActSci), Nathalene Fong (3A CS), Barb Palmer (3A AM/CS) and Sherry Hedden (4A Gen'l). Things on the agenda this term are placement stats (as of May 7, 3027 total placed, 268 still to go), reviews of various booklets, lateness policies, work report guidelines and a new confidentiality policy – note that Coordination can no longer give out phone numbers for co-op students (due to a change in university policy), which makes changing interviews tricky.

Also note, if you did not fill out a white change of address card at your return to campus interview, please do so at the Registar's office. Your temporary address is **not** kept from term to term. The information on it is not used for official material, but it is useful to coordination, especially during interviews.

I tried to make this short and semi-sweetm; sorry if I didn't succeed. Good luck to those going through interviews this term, and I'll catch you later.

-BP

Math presents ...

David Wilcox

June 8, Fed Hall tickets: $6.50, $7.50 for non-Feds Available at MathSoc and the Fed Office

ISSN 0705–0410

mathNEWS is a bi-weekly, sometimes triweekly, publication funded by, but otherwise independent of, the Mathematics Society at the University of Waterloo. Content is the responsibility of the **mathNEWS** editor. Any opinions expressed herein are those of the authors and not necessarily those of MathSoc or **mathNEWS**. Send your correspondence to: **mathNEWS**, MC 3036, University of Waterloo, 200 University Ave. W., Waterloo, Ontario, Canada, N2L 3G1 or to userid mathnews@watdcsu on USENET.

Managing editor: fractious dan schnabel

MathSoc Notes

- The results are in for our third year reps: Ilia Sawitzki, Sue Olin, and Barb Palmer. We got over 50 percent of the possible voter turnout, which is pretty amazing. Ilia topped the votes, well ahead of the rest of the field; Barb, Sue, Karen Thompson and Melissa Janes followed with 5 votes difference between them all. Even Nat Fong and John Omielan beat the number of votes for two of the three previous reps. It was a close contest (requiring two recounts), and I hope all will continue to be involved with MathSoc.

- It may be confusing to see that there are three instead of two third year reps. It was discovered that the class was large enough (over 250) to merit three reps. So, should nineteen 3B students merit special representation? Technically, there shouldn't be 3B or 2A students on campus during the summer, but due to transfer credits and failures there are. It may not have caused any debate if the 3Bs had been included in the 3rd year nominations and voting initially. However, voting priveleges were only given the day before the election, making it too late to run; some 3Bs didn't even know they could vote. So, I think the main gripe was not the lack of a particular 3B rep, but rather the way it was handled.

- The 4A representatives were acclaimed: Carole Coutu and Diane Kilcoyne. For the 1B and 2B classes the reps are as last term: Dwight Ferguson, Andrew Bornyi and Lisa Mesic for 1B; Alexa Clark, Brett Martin and Bill Tilford for 2B.

- Two weeks ago the "office staff" bade farewell to our secretary, Kim DeScally, with pink tie cakes and a small gift. Kim has moved to a full-time job at Needless Hell, and has been missed by all (especially by Jack, who has been doing some of her work). We will soon welcome Anne Fougere to the secretarial job.

- The calendars on the MathSoc wall are filling up with events so fast that it's hard to find dates for new ideas or time to publicize them. The following events have been approved:

  Friday May 24: Road Trip to "The Late Show", Niagara Falls, NY. Tickets are $12 — leave at 6, leave NY at 3am. Proof of age (19), and citizenship is a must. (We've had to leave non-Canadians at the border before!)
  Saturday, May 25: Car Rally. Forms in MathSoc, or talk to Brett Martin. Starts around 1 pm and ends around 6 with a cheap BBQ.
  Friday, May 31: "Math Backyard BBQ" at the Bombshelter. Starts around 3; more details later.
  Saturday, June 8: Pub with David Wilcox at Fed Hall. Tickets are $6.50 for feds, but went on sale Wednesday and might be sold out by the time you read this!
  Saturday, June 15: Road trip to Canada's Wonderland; about $15 including bus, admission, rides. More details to come.
  Saturday, June 22: British Pub Night at Fed Hall. British food, British beer, British Petroleum, Irene & Carla from the Brunswick House.
  Saturday, July 6: Notorious Wine & Cheese.
  Saturday, July 13: Faculty-Student Picnic.
  Friday, July 26: End of Term Pub.

  With so many events, we desperately need help with publicity. So anyone who wants to draw, paint or put up posters, come visit the office!

- Sometime soon we are supposed to get a new photocopier. There were many problems with the present one, especially the quality of copies, so last term's council ordered a new one for the beginning of May. So where is then, you ask? Someday soon ...

- Joy, oh joy — my first council meeting, which was mostly approving various new members and fund for the above events. There was a long debate on lounge renovations, which turned into a heated debate on smoker's versus nonsmoker's rights. You see, last term's council approved a plan to spend about $16 000 on renovating the smokers' lounge on the 3rd floor; it raised the money on the condition that the lounge would be designated non-smoking to save the furniture. Yes, the smokers deserve a lounge, but there is no place for it right now. The ventilation is too poor for a plan to split the existing lounge, but there should be a better place for smokers than the hallway. For arguments on either side, see the March 29 issue of mathNEWS (Vol. 37 #7) — I don't want to start any new arguents.

- You might be able to tell that the Math Society is very busy. We still need help for office hours, publicity, mathNEWS, etc. Help!

- BP

Prez Lida Sez

Quite a lot has happened in the last two weeks. Our social calendar is full thanks to our new social director, Al Laflamme. Al was one of those who answered the ad in "MathSOC presents...." He has been on the job two weeks and has already arranged two pubs (David Wilcox, June 8th among them), a barbecue at the Bombshelter and tonight's road trip to the Late Show (buy your ticket if you don't have one). Come into the office, check out the social calendar and fill in your own calendar.

Because of the social events Jane Dunlop, the publicity director, is swamped with demands for posters. We had people coming into the office with offers to help (thank you) but we can always use more sign painters.

As well as social events, other planning has been going on. Lounge renovations were approved at the last MathSOC meeting. There was some discussion because of the non-smoking issue, however, in the end, council felt that we should go ahead. It will be brown, with couches like those in Fed Hall, carpeting and curtains. Finally a nice place for undergrads to use.

We welcomed a new secretary to the MathSOC office yesterday. Anne will be in 9 - 12 Monday to Friday, stop in and introduce yourself to her.

Again, we always need people. Quite a few people have stopped in to offer to do an office hour or to do anything else that needs doing. As usual we can always use more. Come in to MC 3038, introduce yourself and lend a hand. It is always appreciated.

Lida Cepuch

Mathematical Recreations - Part 1

Magic Squares

A magic square consists of a number of integers arranged in the form of a square, so that the sum of the numbers in every row, column, and diagonal is the same. If the integers are the consecutive numbers from 1 to n^2, the square is said to be of the nth order, and it can be seen that in this case, the sum of the numbers in every row, column, and diagonal is equal to $n\frac{n^2+1}{2}$. In this article, I will consider nth order squares.

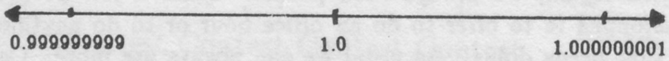
Although there are many different methods for constructing magic squares (including trial and error), I will describe a general method, due to Frenicle, of constructing a magic square of any order. Using this method, to form a magic square of the nth order, we first construct a magic square of the $(n-2)$th order, add to every number in it an integer, and then complete the border with the remaining numbers so as to make it a magic square. This method will become more clear with the example shown in Figure 1, where n = 7 is built up. First, the inner magic square of the $(n-2)$th order is built up in any fashion (including using this method on a magic square of the $(n-4)$th order): the sum of numbers in each line is $(n-2)\frac{(n-3)^2+1}{2}$. To every number, $2n-2$ is added: the sum is now $(n-2)\frac{n^2+1}{2}$. The numbers not used are $1,2,...,2n-2$ and their complements, $n^2, n^2-1, ..., n^2-2n+3$. These numbers are placed at the $4(n-1)$ border cells so that the complementary numbers are placed at the opposite ends of the rows, columns, and diagonals: this makes the sum of the numbers in these lines being $n\frac{n^2+1}{2}$. The only thing left to do is make the sum of numbers in each of the border lines also have this value: this is easily done by trial and error. If the square is built up border by border in this fashion, then the resulting magic square will have the property that if each border is successively stripped off, the resulting square will still be magic.

The above information was obtained from:

Ball, W. W. Rouse, "Mathematical Recreations and Essays", The Macmillan Company, New York, 1956, pp. 193,200,201

The Mad Irishman

46	1	2	3	42	41	40
45	35	13	14	32	31	5
44	34	28	21	26	16	6
7	17	23	25	27	33	43
12	20	24	29	22	30	38
11	19	37	36	18	15	39
10	49	48	47	8	9	4



Now when your eyeball to eyeball with the real line you can call **Complex NumberSystems Limited** for a new direction.

Feedback

To the Gridword Designer:

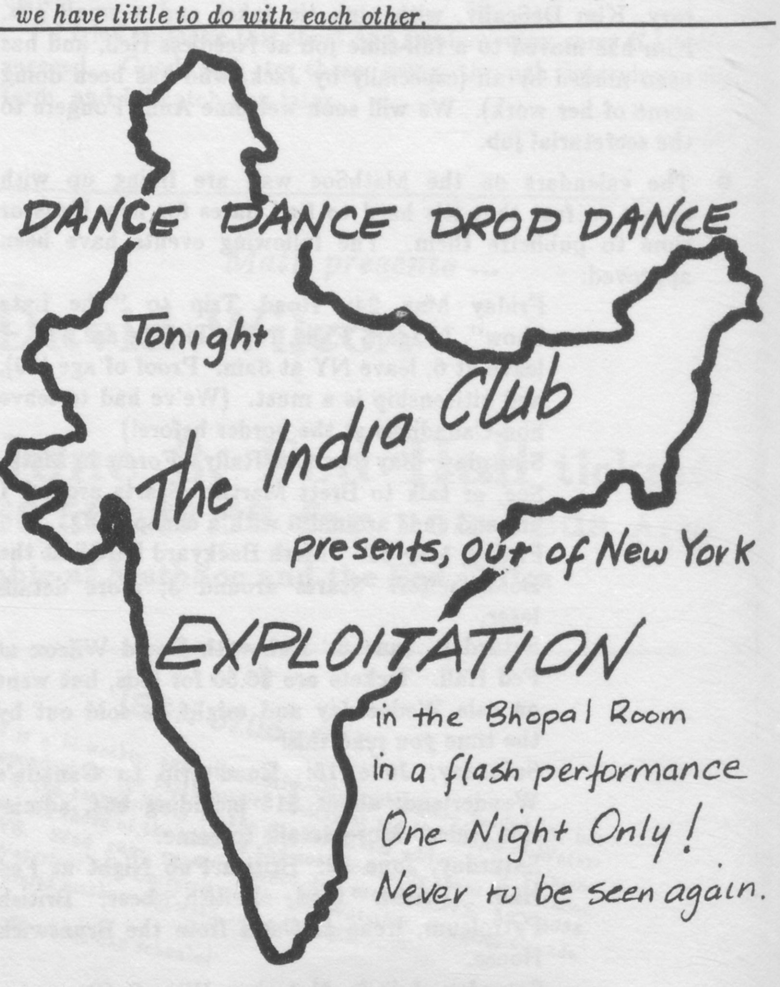
I have two words for you. Challenging and frustrating. The first refers to something which requires some effort to complete, but can be done by non-Himalayan hermits. The second, which aptly describes this past issue's gridword, refers to tearing one's hair out and swearing up and down that the drugs heroin or LSD were deeply involved in the construction of the puzzle.

Now here's a tricky question. Which of the above two words should be applied in order to get people more interested in the gridword? I for one have no motivation to try a gridword that I will throw away with 2 letters on it. (A token giveaway clue, no doubt).

If you have trouble with normal coherent thoughts, try getting some hints from a book on the subject, but don't torment us with puzzles solvable only by someone on the same astral plane as yourself. This is but one more factor contributing to the 'clique' image of MathSoc. Get on the ball, and get people interested, not confused.

4A Flame

Editor replies: Our gridword designer is not an old pro but he is trying. I certainly agree that his last gridword was difficult but i have always found them difficult so i thought nothing of it. This week's is hopefully easier - i think it is. By the way, don't let ***mathNEWS*** *contribute to your image of MathSOC - we have little to do with each other.*



How Coastlines Got A Dimension of 1.2

Before I actually explain the bit about coastlines on this planet having a dimension of 1.2, permit me to wonder aloud (in print, actually): Imagine somebody playing Asteroids or some similar game in the Campus centre, banging the hyperspace button when things get tense, and subsequently finding himself (I don't say 'him/herself' since it is a documented fact that almost all videogame players are male) playing the same game in an arcade in suburban Seattle.

Now, back to the topic that I haven't left yet because I haven't gotten to it yet, except for the title (uncryptic by **mathNEWS** standards) which doesn't really count. This article is about squiggly things called "Fractals," which can best be defined as squiggly things. Most things in the real world are squiggly, and until recently geometry had very little to do with describing this "real world," Descartes notwithstanding. The last time I saw a mountain, it was not perfectly conical, and the average cloud is not spherical. So, mathematicians being the wise and not-quite-all-knowing-but-getting-there-quickly people they are, fractals were invented as a way to describe the world of physics.

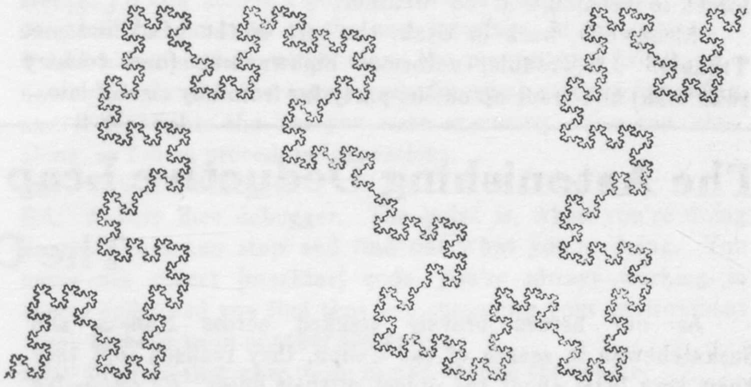
You can usually identify a fractal by how squiggly it is, but mathies usually prefer to quantify vague terms like squiggly. In this case, some person (probably and ironically, he/she must have been very removed from the real world) thought up non-integral dimensions for describing squiggliness. The simplest example that is most often used to illustrate the concept of "weird dimensions" is a stretch of coastline. For example, how long is the west bank of Laurel Creek from the point it enters the triple-U campus to the point it leaves? The answer is, "It depends." If you were to go measure it with hip waders, duck repellent, and a five-metre stick to measure from point to point, you might come up with 2 or 3 kilometres. On the other hand, say you were very patient and remeasured it this time with a one-metre (or even one-centimetre) stick, you would get a considerably greater length. If this is not obvious, consider any 5-metre length that you measured the first time. In fact, the path the bank takes between the two endpoints of this interval will not be very straight. Most likely, it will meander quite a ways to the left and right, backtracking occasionally as well. If you use the increased resolution of a one-centimetre measure, this 5 metres may well come out to be closer to 50 metres! This, of course, applies to every 5-metre snippet of Laurel Creek, and the same argument can be applied to the one-centimetre lengths *ad infinitum*. Thus, the length of the west bank, etc., is infinite!

What now? Intuitively, Laurel Creek is shorter than the Amazon, but mathematics seems to dispute this. Here is where the fractional dimensions come into play. Consider a "normal" figure, say a square. How many dimensions does it have? "Two," I prophesy that you are saying to yourself. For the purposes of analogy, consider its length, area, and volume (Just because you're paranoid doesn't mean nobody's following you!). A square has infinite length, zero volume, and "reasonable" area. Call these 3 words 1-D measure, 2-D measure, and 3-D measure. Now its 1-D measure (using a 1-dimensional "yardstick") is infinite, and its 3-D measure using a 3-D "yardcube" is zero (i.e. infinitely many yardsticks fit in a square, and zero yardcubes fit in a square). Thus, it would seem reasonable to conclude that a square has dimension 2. Fortuitously, an integer happened to be between 1 and 3 in this case; but what of Laurel Creek? Applying the same methods, its 1-D measure is infinite, and its 2-D measure is zero. Thus its dimension lies somewhere *between* 1 and 2, probably about 1.3.

A more formal definition of "dimension" in this sense runs as follows. For any geometric figure, it has a dimension L such that for all dimensions d<L, the figure's measure in that dimension (not necessarily an integer) is zero, and for all d<L, its measure is infinite. Only using the dimension L can measures (read "lengths of rivers") be reasonably compared. It has been empirically determined that the average dimension of coastlines is 1.2.

As a pretty example of filler in **mathNEWS**, here is a well-known geometrical fractal that some of you mathies sitting bored at the back of a CS140 M1 class can devise a computer program to draw, if you can figure it out. (Big hint: recursion is almost essential.) (Even bigger hint: If you're *really* bored, try drawing it by hand.)

Center of Gravity



Classified

Impersonals

Handsome, intelligent derfy looking for derfyiette (no, center of gravity, that is not something that I will use to wipe my mouth with) of my dreams. Desired qualities (in order of importance) are : female, human, alive (no cadavers please !), has no grandchildren, intelligent (preferably more than I am) (that won't take much - d.ed), plus the rest of the usual attributes of a budding beauty pageant queen.

Does Bob really know ConEuc, or is he still programming in FORTRAN?

Wanted: Lots of used TS1000s, ZX81s and a black and white TV (used). Will pay cash for that mouldy black square frisbee gathering dust in your closet. Contact Center of Gravity at **mathNEWS** ASAP.

Bob: See fork(2).

The Caliph of Caliphornia

When we left our illustrious heroes they were on the shores of one of the lakes in Nevada, travelling on foot because the last of their scooters had died miles from any BP station. Onwards they trudged, through lakes, around muddy shores, and over marshy swamplands. While they fought off mosquitoes, Centre of Gravity proved that the Caliph eats quiche.

Finally they reached the open plains of Utah. Somewhere ahead of them lay Caliphornia, the state they sought. (Those who sought the state of Nirvana were out of luck.) But the doughty Irishmen, Paul O'Beda and Mad John O'Melian, had disappeared. Unbeknownst to their companions, the forces working against **mathNEWS** had lured these two mighty warriors astray to the pleasure palaces of Las Vegas, where they cavorted merrily.

Back in Waterloo, derfy, monitoring the situation, realized that he must act. Rushing to the secret **mathNEWS** airport, he boarded the secret **mathNEWS** jet, and hurried to Las Vegas to pick up the wandering Irishmen, cary them to their companions in Utah, and return himself to Waterloo to continue his monitoring. Unfortunately, a horde of men armed with machine guns hijacked derfy's plane to Havana, where he was forced to disembark in -30° weather.

Meanwhile, back in Utah, the rest of the band had met Trouble. J.G.Trouble, notorious highwayman (and country road man) had crept up on the party far from any sign of law.

"Hand over yer idears now, nice an easy, an we won' have no trouble. Har har." said Trouble and his seven sidekicks in unison.

But our protagonists were not so easily taken.

"What should we do now?" they asked dan. "What can we do without the strength of our Irishmen?"

"We fight. Draw your weapons."

While Stewart (absent) hastily sketched a detailed diagram of a tank convoy, the others began to fight. Trouble and his men proved too slow on the draw for **mathNEWS**'s seasoned x-acto knife experts. They had been hacked to pieces and were almost ready to surrender when the local Shirriff arrived.

"What are your names?"

"We are **mathNEWS**!"

"What is your quest?"

"We seek the Holy LaserWriter."

"What is your favourite colour?"

"PINK!!"

"Do you mind if I join you?"

"Not at all. Come along."

And so our heroes headed on into the sunset, towards the renowned Sesame Institute, where they intended to ask for advice from the experts. O'Beda and Mad John still frolicked in Las Vegas, while derfy froze in Cuba. Will they be able to regroup? Will they reach the Sesame Institute? Can they get the LaserWriter? And what if they meet ... the Caliph!

Tune in next issue, as our protagonists reach Caliphornia.

The Astonishing Deductive Leap That Showed How To Find The Caliph

As our heroes bravely trekked across Kansas and Saskatchewan in search of the Caliph, they realized that they knew very little about the object of their quest. By discussing this fact amongst each other, they came up with this line of reasoning:

"We know very little of the Caliph. Therefore he is mysterious. But we do know of his existence. Thus he must be the cause of this mysteriousness. Ergo, he doesn't want people to know what he is doing. Hence, he must be doing strange and wonderful things of great wisdom. He is also known as 'The Caliph of Caliphornia.' From these last two statements, it follows that he works for Apple in their secret lab deep inside Mt. St. Helens."

"Well," dan said in deep tones of commanding bewilderment, "How do we find him deep inside this volcano? Surely there isn't a doorbell at the side of a lava flow?" "Who knows," Alfred mused. "This Caliph guy is quite a character." This set yours truly to thinking as follows.

The Caliph is unknown to us, and we are Mathies. Now all Mathies are very familiar with letters in many alphabets, from proofs in abstract algebra. For the same reason (as well as APL) we know of diverse strange symbols. On the other hand, the knowledge dealt out within the gray walls of Castle Waterloo is so abstract that its inhabitants almost never encounter actual numbers. For these two reasons, and also since the Caliph is a "character," the process of elimination leads to the conclusion that the Caliph must be a number. Continuing, the only pointless thing that Mathies do is integrating weird things like the root of *tan*x, and we Mathies are searching for the Caliph, which would be pointless if the Caliph were not real but imaginary. Thus the Caliph must be real and (since he is a number), therefore he must be a real number.

From this conclusion, as has been proved dozens of times in this hallowed journal, it immediately follows that the Caliph eats quiche.

"Thus," I exclaimed to my esteemed colleagues, " we must devise a way to detect quiche. The Caliph of Caliphornia will soon follow!"

Center

Mushed head.
I've lots of room
to write so i'll
be brief. Two
computers stopped
talking to each
other so mathNEWS
ended up 40 minuits
behind schedule. So
we all were kinda
tired when we
finished this and
some lines weren't
as straight as
they could have
been and a lot
of bad jokes
were dropped.
Thank go out
to all of the
3-d staff here
at mathNEWS.
They are:
Derfy - who's
learning to eat
pizza as we
laugh at his life;
Center - whose
humor knows
no dimension;
Bonita - who
never heard us
laugh at her;
The Mad Irishman
who did a little
of everything and
a lot of writing;
Cary Timur -
Caliph before
PM 3:52

continued elsewhere

The mathNEWS Interview

This week we spoke with Bob Atkinson, 3A Pure Math, who has just returned from a work term at Xerox's Palo Alto Research Centre in Palo Alto, California. We thought we'd ask him about what PARC is like, how co-ops go about getting jobs in a U.S., and about Smalltalk, a programming system developed at PARC. If you have more questions, you can usually find Bob hanging around the Computer Science Club (MC 3037), or not.

mathNEWS: Why did you decide to work at Xerox?

Bob Atkinson: Because it's a neat place. Xerox PARC has been doing a number of things I find interesting. I was personally exposed to the environment I working in through a friend of mine, Mike Rutenberg, who worked down there in high school. (He took the last half of Grade 13 off and worked on Smalltalk.) Now, Smalltalk grew out of a vision of what personal computing could be, and they coined the term 'Dynabook' to represent that vision. A Dynabook was a personal computing machine with an incredible amount of computing power; it was envisioned to be the size of an 8½ by 11 notebook.

mN: Something you could easily carry around.

BA: Exactly. You would do much of your daily tasks that you now do on paper through this medium, which would be connected via some networking device to other people and other Dynabooks. With this vision in mind the Learning Research Group started working on an environment which would be the software for this machine.

mN: And was it the 'descendent' of this group that you worked in?

BA: Yes, that's where I was. It's a small group of about twenty people that has evolved about a few people that've been there since it started. Some people term it the 'Smalltalk Group' but it's really the System Concept Laboratory.

mN: What would you say is the basic premise of PARC itself?

BA: Xerox has taken a really hands-off approach to it. They've basically set up these people, some really smart people, and said "Go off and do neat things." Xerox has been somewhat criticized for not taking very good advantage of the technologies that have come out of PARC. PARC, for instance, developed laser printers. The group I was working with was one of the first to experiment with multiple overlapping windows.

mN: That we now see on the Macintosh?

BA: Yes. Apple has taken very good advantage of Xerox technology, and marketed it quite well. Steve Jobs, president and founder of Apple, once termed PARC "a great national institution." Xerox management didn't take kindly to this attitude, but it's not an incredibly bad statement, in that they are reasonably open and there's quite a close co-operation between them and a large part of the academic community. They've got a very close association with Stanford, and play an active role in SIGPLAN and the ACM [Association for Computing Machinery].

mN: What are your impressions of Smalltalk as a programming language?

BA: It's hard to separate Smalltalk the language from Smalltalk the programming environment. One of the things that makes Smalltalk different is that it's object-oriented. Mumble. In CS 340 you meet with the concept of abstract data types, a way of bringing together a set of operations on some information that has an abstract, mathematical form. You might create a set of procedures and a set of type declarations that represent the concept of a set, which you might add elements to, intersect, unite with other sets, or test for a certain element.

In Smalltalk everything is an abstract data type, though they term them 'objects'. Computation is performed by sending messages to these objects. So evaluating the expression '3 + 4' would send the message '+' with the argument the object '4' to the object '3', and this object would be responsible for implementing the message '+' and it would be up to it decide how to respond to that message. (It just so happens that '+' sent to '3' does in fact add the two numbers.)

All objects are *instances* of *classes* of objects. You look in the object's class to find how to respond to messages sent to that object. You could create a 'set' class and implement 'plus' in 'set' class to unite the receiver of the message and its argument.

This probably sounds like a mundane idea. The thing about the Smalltalk system is that absolutely everything in the system is an object. Integers are objects, floating-point numbers are objects, sets are objects, even the stack frames that implement the computation are objects. It's this complete uniformity that makes it a very nice, malleable system. For instance, I'd run across a piece of software that I didn't like — someone had screwed up the user interface, in my opinion. I would hit control-C, which stops the process and brings up a new window, with the source code for what you are executing, and it highlights the line you were executing. You can 'step' along, or follow procedure invocations, ...

mN: This is a debugger?

BA: A very nice debugger. The point is, when you're doing anything you can stop and find out what you're doing. You never see object [machine] code, you're always working in source code, and you find that you customize your environment much more than in another system.

mN: It's just that easy to go in and change the source.

BA: Yes, you never work in anything but the source code. The Smalltalk system exists as a great big morass of objects — the typical image has about 40 000 objects lying around. All Smalltalk is is this collection of objects. You basically program by patching objects or adding objects onto the side.

mN: Would you consider the Smalltalk approach the ultimate extension of modular programming?

BA: It certainly does a lot nicer job of it than most other things. It's not perfect, it's not ultimate — I know lots of places where I'd like to change things.

mN: Can you see Smalltalk migrating? Or, can you see many programmers using it in the future?

BA: One of Smalltalk's troubles is that it uses a heck of a lot of processing power. There's no way you would even consider running it on, say, a time-sharing VAX. One of the reasons for this is that it does a lot of things for you that other systems don't do. Another is that all procedure calls are bound at runtime — you don't know, until you actually send a message to an object, what piece of code is going to be executed.

mN: Is it possible that Smalltalk will become commonplace?

BA: Yes, it is. You're not going to see it on anything but a personal machine with not less than two megabytes and nothing less than, say, a 68000 [The Motorola MC68000 microprocessor — used in the Mac and Lisa.]. There a couple of implementations on 68000 that run at quite acceptable speeds.

continued on page 8

continued from page 7

Currently the smallest machine you can get is a Tektronix machine which sells for $14 000 U.S., but Atari is soon to be releasing a new personal micro, 68000-based, which sounds to me like it could make a very good Smalltalk machine.

mN: Once the technology arrives, will there be a Smalltalk revolution, or maybe just a Smalltalk wave?

BA: I don't know if there's going to be anything like that. It's a different philosophy of doing things and it allows you to do somethings easier than in other systems. It's very easy to whip up prototypes for conceptual interfaces, far easier than in anything else I know, because a large part of the machinery is already there and you just modify it. I'm spending my summer working on Maple for the Tektronix, bringing up a prototype user interface.

"Smalltalk revolution" – I won't hold my breath. Hopefully some good ideas from it will percolate into other systems.

mN: Sometimes co-op students say that they've worked on machines X and Y and written in language Z, but could you crystallize something and say you learned *that* at Xerox?

BA: Perhaps I've begun to appreciate the value of having a computing environment where things are not hidden away from me. If you have a bright new idea of improving something you can do it and contribute to the evolution of that system; whereas if things are hidden from you, you have no vehicle for experimentation or creativity, and it's up to some wizard who probably doesn't have time. I've learned to be less tolerant of closed, "you-only-have-access-to-what-you-barely-need-to-be-able-to-do-what-you're-supposed-to-be-doing"-type attitudes.

mN: How does the department of Co-ordination and Placement regard your term at Xerox? Is it a proper work term?

BA: Oh yes, I did a work report, I actually had a co-ordinator, though he didn't come and visit. It was just like finding your own job anywhere else. There some finangling I had to go through to get a work visa. (Waterloo has an exchange program with Northeastern University.) Unfortunately visas are very tight – there are none left for this year, and only ten come for the whole year each July. You *can* try to get one through U.S. Immigration, heaven help you. You can try to go through UW, which used to be a much better way of doing things, but relations have become somewhat sour between Canada and the U.S. in recent years. There's another international organization, I.A.E.S.T.E., which helps students co-ordinate practical training in a large number of countries. Canada is in U.S.'s bad books because many Canadians go to the U.S. for technology but no-one comes in the other direction. These programs have work on a reciprocal basis, and that's why visas are drying up.

mN: Are you looking forward to going back to California?

BA: Oh, very much. I had an absolute wonderful time. The people I worked with were incredible. I should point out that I was in Northern California where it's cooler. I actually had to scrape some frost off my car once. There's a lot of people in that area. I'm from Winnipeg, which is not a very big place, and just outside the city you're in wheat fields; whereas you've got people strung all the way along the Bay area, which is 45 miles deep. I felt crowded.

Alternate Uses of Math - Part 1

Cryptanalysis

Occasionally, people have secrets that they want to keep (e.g. the army). Thus, they want to make their written messages unintelligible to all but the appropriate recipients. The general techniques used to accompish such a purpose, i.e. the hiding of the meaning of messages, constitute the study known as "cryptograpy". However, if the message falls into the wrong hands, the person(s) will try to decode the message, but without knowledge of the cryptographic details employed. Efforts aimed at reading a secret message in this way comes under the heading of "cryptanalysis". This article will describe a very simple encryption technique and how to analyse it.

I will consider a method of assigning letters of the alphabet (a,b,c...z) to different letters of the alphabet. One can generate the assignment rules by randomly assigning a letter to A, a different letter to B,..., the last remaining letter to Z. One can represent these substitutions by a "substitution alphabet" as shown below:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	L	V	C	H	K	Q	U	E	O	X	R	P	T

Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	A	F	J	S	M	D	Y	G	Z	I	N	W	B

The upper line is the letters in the real message, called the "plain sequence", while the lower line is the letters of the coded message, called the "cipher sequence".

However, the problem is being able to remember the code. However, if it is written down, it could be lost or stolen. Thus, I will consider a technique that only involves memorizing 2 numbers.

First, transform each letter to its position in the alphabet (i.e. A -> 1, B -> 2,..., Z -> 26). The result is a set of numbers from 1 to 26. The encryption technique will involve assigning to each of the numbers 1 to 26 inclusive a unique number between 1 and 26 inclusive (i.e. don't use any number twice - if you do, then the resulting encoded message can be decoded in more than one way!). The method that will be discussed here uses a linear transformation. Let $A = \{1, 2, 3,..., 26\}$. Consider the relation $C = aP + b$, where a and b are positive integers and P consists of elements in A. Calculate C for all elements of A. Take the residues of C (i.e. the remainder when C is divided by 26, with a remainder of 0 being taken as 26). They will form a set of numbers with values between 1 and 26 inclusive. For each residue of C to be distinct (i.e. 1, 2, 3,..., 26 in some order) requires only that a and 26 be relatively prime (i.e. a is not a multiple of 2 or 13). Convert the residues of C to letters (i.e. 1 -> A, ...). For example, take $a = 3$, $b = 2$. The sustitution table now becomes:

plain letter	A	B	C	D	E	F	G	H	I
plain number	1	2	3	4	5	6	7	8	9
residue	5	8	11	14	17	20	23	26	3
cipher letter	E	H	K	N	Q	T	W	Z	C
plain letter	J	K	L	M	N	O	P	Q	R
plain number	10	11	12	13	14	15	16	17	18
residue	6	9	123	15	18	21	24	1	4
cipher letter	F	I	L	O	R	U	X	A	D

continued on page 9

continued from page 8

plain letter	S	T	U	V	W	X	Y	Z
plain number	19	20	21	22	23	24	25	26
residue	7	10	13	16	19	22	25	2
cipher letter	G	J	K	P	S	V	Y	B

If the message to be encoded was:

The next issue of mathNEWS will be available two weeks from today.

then the encoded result will be (making everything uppercase):

JZQ RQVJ CGGMQ UT DEJZRQSG SCLL HQ EPECLEHLQ
JSU SQQIG TDUO JUNEY

Analysis Technique

This type of encryption is usually solved by considering frequency distributions. Not all letters of the alphabet are used with equal frequency. The following gives the frequencies of letters of the alphabet in a sample of 1000 letters, arranged alphabetically and by frequency.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	73	9	30	44	130	28	16	35	74	2	3	35	25

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	78	74	27	3	77	63	93	27	13	16	5	19	1

Letter	E	T	N	R	I	O	A	S	D	H	L	C	F
Frequency	130	93	78	77	74	74	73	63	44	35	35	30	28

Letter	P	U	M	Y	G	W	V	B	X	K	Q	J	Z
Frequency	27	27	25	19	16	16	13	9	5	3	3	2	1

Similar frequencies should occur in the encrypted message, but in a different order. The distribution of frequencies in the sample encrypted message above is:

Letter	Q	J	E	S	G	U	L	C	Z	R
Frequency	8	5	5	4	4	4	4	3	2	2

Letter	T	O	H	V	M	P	I	D	N	Y
Frequency	2	2	2	1	1	1	1	1	1	1

If we assume that the most frequent letter $Q_{C4} = E_{P4}$ and that the second most frequent letter $J_{C4} = T_{P4}$, then it is likely that the cipher JZQ is THE. This tentative identification of three letters

Cipher	Numerical Equivalent	Plain	Numerical Equivalent
J	10	T	20
Z	26	H	8
Q	17	E	5

gives rise to three congruences involving their numerical equivalents. These values can be substituted into the congruence relation:

$C \equiv aP+b \pmod{26}$
(This is how the residues were originally obtained.)

to give the following three relations:
$10 \equiv 20a+b \pmod{26}$
$26 \equiv 8a+b \pmod{26}$
$17 \equiv 5a+b \pmod{26}$
If we subtract the third congruence from the second congruence, we obtain:
$3a \equiv 9 \pmod{26}$
$a = 3$
We use this in the third congruence to obtain b:
$15+b \equiv 17 \pmod{26}$
$b = 2$
These values for a and b are of course the values used in the example.

There are other techniques that could be used to help find the encryption technique (e.g. using frequencies of the first and last letters of words). However, most of these technniques requires that the encrypted characters be separated into words. To make it harder to decipher, the words can be compressed together. To test what you have learned, attempt to decipher the following message that has been encrypted using a linear transformation.

```
USDCL   QPEZQ   PGSDA   MSERQ   TYVEA   PASZT
DULMH   PYJOY   AAQCY   PRYDY   XPGAA   EYSNO
IAIGZ   ZJYAU   LGFYQ   DSPRY   LOSLY   GDPYL
CYDUL   MHPGS   DPYUR   DGWEY
```

The solution will be printed in the next issue of **mathNEWS**.

The above information was obtained from:

Sinkov, Abraham, "Elementary Cryptanalysis", Random House, 1968

I am planning to write a series of articles on interesting applications of mathematics. If you have anything that you want to read about, or think that other people will want to read about, please submit them to the **mathNEWS** box on the third floor.

The Mad Irishman

Cary's classic rival,
Tom Ivey - the only
person who thinks
about mathNEWS
before production
night and can
therefore do interviews
and endanger his
life by doing the
gridwords. Tom
does a lot for
mathNEWS but that
doesn't mean you
shouldn't knock him
about when his
gridwords became
too obscure.
Thanks also to
other people who
helped make mathNEWS
what it is. They are:
The unabridged Bob
Atkinson, who gave
us an interview
while double PARCed;
4A Flame who
burnt up Tom a
bit;
BP who keeps
us in touch with
the outside world;
and of course
Lida Cepuch,
the prez, who
although cute
and in spite of
her good taste
cannot be
forgiven for even
considering to
get Cary's help

continued elsewhere

Doctor Tongue's 2-D House of Gridwords

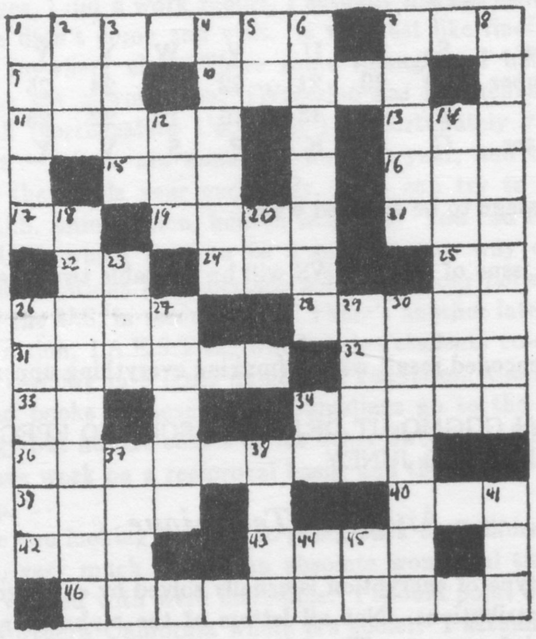
Well, so far nobody has handed in solutions to last issue's puzzle, but we'll tell you the answers anyway. (By the way, we apologize for the unexplained absence of a clue for 21. down (This probably made the puzzle a bit hard (See the Feedback from 4A Flame), so we're toning this one down a might.)) Submit your solutions some time before next issue to the *Black Box* in the 3rd Floor lobby of MC.

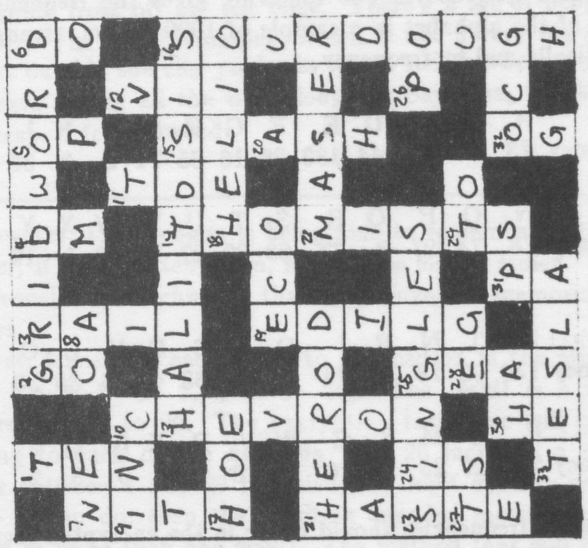
Across

1. Give words, Richard
7. one of Glorfindel's kin
9. beware that we exist
10. you're lax with Frankie
11. legless reptile juice
13. white clerical garb
15. see it, lo, the motor oil
16. bovine beckon
17. anti-imperialist system
19. source of salty river
21. ours is class G
22. bondage Doctor
24. French ruler
25. Systems Analysis
26. draw acidly
28. of citizens
31. flip the Boolean
32. white metal
33. behead the hag
34. slime molds, etc.
36. "Club" movie
39. Oz's Bert
40. is to circle as segment to line
42. and so forth
43. waste metal, junk
46. loafer's laneway

Down

1. ICR's sod-turner
2. anger, wrath
3. endangered copper species
4. chain mail, plate, etc.
5. Fr. pronoun
6. snappy collision
7. august trials
8. let's get series
12. geritol, defer to elders
14. de-de-lousing
18. social event for 1B mathies
20. small firm
23. not in mathSOC, go check the CSC
26. make Cain's brother ready and willing
27. it's a good point, his horrible hat
29. backwards with Banshees
30. let it age on the vine
34. a long, long way to run
37. reverse those backache problems
38. Kid Carson and the Pen Gang, headed for Feb. show(down)
41. scan for felines
44. much less than Fortran
45. salute Billy with a fish-stick





for her Phil 140 assignment.
Once again - thanks to all, and especially those who i've forgotten.

mathNEWS plug: we can always use more ~~money~~ help so come on out and meet interesting people (see LOOK AHEAD for exact dates).

Drop any submissions into our black box on the Third Floor.

I am the editor, dan schnabel, so yell at me if your not happy, but i think you will be.

Good night.

Witches, Warlocks and Toaster Ovens

by Rodney Badchef

The first nonfiction attempt by this reknowned author of many novels dealing in the occult is a masterpiece. No other work to date separates the myth from the fiction. This volume is an entertaining, colorful, thought prevoking and often frightening account of the work of wizards in this techno-toaster era. The chapter on identification of charred heaps and their removal from twisted, oversized cooking trays is, if i may use the words of a collegue, "good."

I whole-heartedly recommend this book to anyone with an amateur or professional interest in the occult, anyone living off campus who can't afford to eat out all the time, or anyone who doesn't have a weak stomach and wants an excellent addition to any book collection.

Rodney Badchef fans will not be disappointed.

"Witches, Warlocks and Toaster Ovens" is published by Random House and sells for $19.95.

I. Emma Masterbaker