Math 103A – Winter,2001
Professor John J Wavrik

Filling In Tables
Cancellation and Backtracking

One often needs, in a computer program, to be able to systematically run through all possibilities to search for cases where a special condition is satisfied. The problem of finding all possible tables that satisfy the conditions for a group can be thought of this way. It is straightforward to write programs to check associativity, existence of an identity, and existence of inverses. Associativity, for example, can be checked using the pseudo-code:

```
associative? := true;
for x in S do
   for y in S do
      for z in S do
            if  (x * y)*z <> x * (y * z)
            then  associative? := false;  exit;
```

If the set S has n elements, this code requires that we check n^3 possibilities if the operation is, in fact, associative.

The problem of finding all groups of order n could be thought of as an essentially combinatorial problem[1]: we are essentially asking how many ways an n x n table can be filled in to satisfy the conditions for a group. There are n^2 boxes in the table – each can be filled in with one of n elements. So we can easily write a program with n^2 nested loops each running through n elements – and then check each table we generate to see if it describes a group. This would mean generating $n^{(n^2)}$ tables.

n	n^{n^2}
2	16
3	19683
4	4294967296
5	298023223876953125

This rate of growth makes this approach totally unrealistic.

Using Theorems:

But we, in fact, do not have to generate complete tables and then check if they satisfy the group theory conditions. There are theorems that tell us something about the characteristics of tables which do or do not define a group. Here is one such theorem:

[1] We shall eventually see other ways to look at this problem.

Theorem (cancellation laws):

If G is a group, x,y,z elements of G then

1. $x*y = x*z \Rightarrow y = z$
2. $y*x = z*x \Rightarrow y = z$

proof:

Since x has an inverse, x', we have $x'*(x*z)=x'*(x*y)$.
By associativity $(x'*x)*z = (x'*x)*y$.
By definition of inverse $e*z = e*y$
By definition of identity $z = y$
(version 2 is similar)

Corollary:

In a group table, the elements in any row or any column must be different.

Backtracking:

What this means, in terms of our problem, is that certain tables can be rejected before they are entirely filled in. For example, if we are trying to find groups of order 3, we may assume that the elements are A,B and C and that A is the identity. This means that we have only to fill in 4 boxes rather than 9.

A	B	C
B	1	2
C	3	4

We cannot put a B in the box marked 1 -- so there is no point in checking any tables that have a B there.

Here is a quick outline of a method, called backtracking. It involves running through the boxes in a specific order (we will use the numbering above). We arrange the things that can be filled into the boxes in order (we will use A, B, C). We put the first legal choice in a box and then go on to the next box. If we reach a box where no choices are legal, we back up to the previous box and make the next choice. If we get to the end, we then back up to the last box where there are more possibilities. The process continues until all possibilities are exhausted. [It is easier to do it than describe it. It is easier to describe it than write code for it.]. The cancellation laws allow us quickly to rule out many possibilities.

As far as we can tell, nothing prevents us from putting an A in box 1. (note that we cannot put a B in this box – and that we have not tested C)

A	B	C
B	A	2
C	3	4

Now let's run through the possibilities for box 2. We cannot put in an A or a B. C is the only choice which gives different elements in the row – but if we put C in box 2 we get

A	B	C
B	A	C
C	3	4

Which gives a duplicate in the last column. We have therefore exhausted all possibilites for box 2 which would be consistent with our previous choice. SO WE BACKTRACK TO BOX 1.

We have just tried an A in that box and found that we could not continue. We rule out B. The only other possibility is C.

A	B	C
B	C	2
C	3	4

Now go on to box 2. There is no visible conflict putting A in this place (and, indeed, only A could go in this place).

A	B	C
B	C	A
C	3	4

There is no possibility except A that will work in box 3.

A	B	C
B	C	A
C	A	4

There is only one possibility for box 4. This leaves the table

A	B	C
B	C	A
C	A	B

There are no possibilities left to examine. This is the only table for a group of order 3.

We have, in essence, just examined all 19683 tables to see which give groups of order 3!

Compare this table with the table for addition of integers mod 3.

0	1	2
1	2	0
2	0	1

These tables are essentially the same. The elements have different names, but there is a one-to-one correspondence $0 \to A$, $1 \to B$, $2 \to C$ which transforms this table to the table above. The terminology we use for this is that the two groups are isomorphic (literally, they have the same form). From the point of view of group theory, the groups have the same properties.

Definition: A group G_1 is isomorphic to group G_2 (in symbols $G_1 \approx G_2$) if there is a one-to-one and onto mapping $\phi: G_1 \to G_2$ so that $\forall\ x,y \in G1$ we have $\phi(x*y) = \phi(x)*\phi(y)$.

If you do the backtracking for groups of order 4, you should discover that there are 4 group tables. Three of these are isomorphic to each other. The third is not isomorphic to the others. We often say, in an abbreviated way, that there is only one group or order 3, but 2 groups of order 4.

To some extend the purpose of this handout is to advertise the amazing power of theory. Use of a rather simple theorem about groups told us something about the characteristics of group tables. This knowledge led us to design a far more efficient search algorithm.

But it gets even more amazing. There is a theorem, which we shall prove shortly, that will allow us to say that there can only be one group of order 5 – without touching a table. (I will leave you to determine, if you are interested in this, how many distinct group tables of order 5 there can be – I only am saying that they are all isomorphic to each other.)[2]

We will do work, this quarter, in showing how a great many ideas about groups can be deduced – how rich the consequences of the group properties are. Even if your interest is mainly in computation and application, you will find theory an important computational tool.

[2] If you are interesting in this, I should warn you that for n=5 there can be tables having A as identity and different elements in each row and column which are not associative. Finding an example of this would also be an interesting exercise.