The Bruck-Ryser Theorem and the Search for a Finite Projective Plane of Order 10

Costandino Dufort Moraites

April 2, 2011

1 Motivations and Overview

Finite projective planes are a less well-understood object than one might expect. An interesting example of this is the case of the Bruck-Ryser Theorem, a theorem which rules out some orders of finite projective planes. For discussion purposes, we state the theorem now.

> **Bruck-Ryser.** *If $n = 1, 2 \pmod 4$, then a necessary condition for the existence of a finite projective plane of order n is that there exist integers x, y satisfying $n = x^2 + y^2$.*

From the statement of the theorem, one can see that 10 is the sum of integer squares, and coupled with a weaker theorem about the sufficiency of certain conditions for the existence of a finite projective plane, for a long time it was hoped that the existence of a finite projective plane of order 10 could fuel a proof of the sufficiency of the Bruck-Ryser theorem. The proof of the non-existence of a finite projective plane of order 10 shattered this hope, and further highlighted the insufficiency of our current understanding of the problem.

In these notes, we will first prove the Bruck-Ryser theorem, then we will try to pinpoint what made proving the non-existence of a finite projective plane of order 10 so computationaly difficult, closing up with further historical remarks and thoughts.

We note that we follow a proof of the Bruck-Ryser theorem laid out in [CAM], and much of the anecdotal information, as well as the discussion of the computational side of the problem was found in [LAM]. Where the two main references fall short is in the discussion offered to explain how the topics discussed sit today after the passage of some 22 years. To this end, I add some of my own commentary based on the availability of computational power today and the clarity of hindsight.

2 The Bruck-Ryser Theorem

The proof uses four facts from number theory which we state below. The facts are fairly straightforward, but proofs can be found in [CAM]. We also define the incidence matrix of a finite projective plane.

Fact 1. The "four squres identity."

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

where

$$y_1 = a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4$$

$$y_2 = a_1x_2 + a_2x_1 + a_3x_4 - a_4x_3$$

$$y_3 = a_1x_3 + a_3x_1 - a_4x_2 - a_2x_4$$

$$y_4 = a_1x_4 + a_4x_1 + a_2x_3 - a_3x_2$$

Fact 2. If p is an odd prime and there exists integers x_1, x_2, not both divisible by p, such that $x_1^2 + x_2^2 \equiv 0 \ (mod\ p)$, then p is the sum of two integer squares. The analogous result holds for four squares.

Fact 3. Every positive integer is the sum of four integer squares.

Fact 4. For any integer n, if the equation $x^2 + y^2 = nz^2$ has an integer solution with x, y, z not all zero, then n is the sum of two integer squares. Said otherwise, the equation has a solution when $z = 1$.

Definition. Let there be a finite projective plane of order n and define $N = n^2 + n + 1$. Then the incidence matrix A of that finite projective plane is an $N \times N$ matrix with rows indexed by points, and columns indexed by lines (or the other way around), with the entry (i,j) equal to 1 if the i^{th} point is incident to the j^{th} line, 0 otherwise.

Proof of the Bruck-Ryser Theorem.

Consider a finite projective plane of order n, where $n \equiv$ 1or 2 $(mod\ 4)$. The number of points of a projective plane of order n is $N = n^2 + n + 1$; and we note that $N \equiv 3$(mod 4).

Let I be the identity matrix, J be the matrix with all 1's, and A the incidence matrix of our plane. Then

$$AA^T = nI + J$$

All this is saying is that when we take the dot product of any two rows, the dot product is 1 if the rows are distinct, and $n + 1$ if the two rows are the same. This is simply from the definition of the order of a projective plane because 2 points are incident to a unique line, hence the 1, and any one point is incident to $n + 1$ lines.

Let $x_1, ...x_N$be indeterminants[1], and let $x = (x_1, ..., x_n)$. Let $xA = z = (z_1, ..., z_N)$; then $z_1, ..., z_N$ are linear combinations of $x_1, ..., x_N$with integer coefficients. We have:

$$zz^T = xAA^Tx^T = x(nI + J)x^T = nxx^T + xJx^T$$

which means:

$$z_1^2 + ... + z_N^2 = n(x_1^2 + ... + x_N^2) + w^2$$

Where $w = x_1 + ... + x_N$.

We take a new indeterminant $x_{N+1}$and add nx_{N+1}^2 to both sides of the above equation. Because of our previous conclusion that $N \equiv 3$ (mod 4) , N+1 is divisible by 4. Write $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (by fact 3) and regroup the terms as below:

Starting with our sum of x_i^2:

$n(x_1^2 + ... + x_{N+1}^2)$ we regroup into 4 term sums:

$(n(x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2) + ... + n(x_{g1}^2 + ... + x_{g4}^2))$ where g is N+1 divided by 4. We redistributed our n so that each sum of four terms has an n which allows us to use the 4 squares identity to obtain:

$$n(x_{i1}^2 + x_{i2}^2 + x_{i3}^2 + x_{i4}^2) = y_{i1}^2 + ... + y_{i4}^2$$

where the y's are linear combinations of the x's. Looking at this back in our original equation:

$$z_1^2 + ... + z_N^2 + nx_{N+1}^2 = y_1^2 + ... + y_{N+1}^2 + w^2$$

Recall that the $z_i's$ and $y_i's$ are linear combinations of the $x_i's$. For each z_i and y_j we pick a unique x_k that has a non-zero coefficient in both z_i and y_j. If the coefficients of x_k are the same in both z_i and y_j we let $z_i = -y_j$ so that we can write x_k in terms of the other $x's$ without cancelling x_k out. In the coefficients of x_k are different, we let $z_i = y_j$ and write x_k in terms of

[1]from Wikipedia. Indeterminant: a variable with no value assigned to it.

the other $x's$. We repeat this process for $i = 1, ..., N$, noting that no z_i is a linear combination of x_{N+1}. We notice that because of our specializations we have $z_i^2 = y_j^2$ so that we can eliminate z_i^2 and y_i^2 from our equation for all $i = 1, ..., N$, leaving us with:

$$nx_{N+1}^2 = y_{N+1}^2 + w^2$$

Reaching this point is exciting because if we can only show that x_{N+1},y_{N+1}, and w are integers, then by fact 4, n is the sum of 2 integer squares, thus proving the Bruck-Ryser Theorem. We show just this.

We recount the key points so far: We have written each x_i except for x_{N+1} in terms of its other $x_i$including x_{N+1}. Thus we have N equations and $N + 1$ unknowns, and we haven't solved for x_{N+1}. Then all the x_i can be written as rational functions of x_{N+1}. y_{N+1} and w are linear combinations of the x_i's so we can rewrite them as rational fucntions of x_{N+1}. Thus we can choose x_{N+1} such that each of x_{N+1}, y_{N+1}, and w are integers, making (by fact 4) n the sum of two integer squares.

This completes the proof of the Bruck-Ryser Theorem.

3 The Search for a Finite Projective Plane of Order 10

So why was finding a projective plane of order 10 so difficult? What exactly were their programs doing over the course of the better part of 3 years?

First we consider how incidence matrices played a role in allowing computers to check out possible candidates, then we explain the source of the initial computational difficulty, finishing off with discussing what sorts of optimizations were done to make the program terminate within the writers' lifetimes.

3.1 Validation

There is an equiavlent definiton of a finite projective plane in terms of its incidence matrix. Let A be a $N \times N$ matrix, with $N = n^2 + n + 1$. A is an incidence matrix iff

1. A has constant row sum $n + 1$.
2. A has constant column sum $n + 1$.
3. The dot product of any two distinct rows of A is 1.
4. The dot product of any two distinct columns of A is 1.

Also we notice how all of these conditions are encapsulated in this equation familiar from the Bruck-Ryser Theorem:

$$AA^T = nI + J$$

where I and J are defined as before.

3.2 Optimization

Now that we have a way of checking a candidate incidence matrix, we give the naive estimate of possible projective planes of order 10 and mention some of the techniques used to trim down the total number of finite projective planes that had to be checked.

A finite projective plane of order 10 has an $N \times N$ incidence matrix with $N = n^2 + n + 1$. Adding to that, for each of the N rows, one must pick $11 = n + 1$ entries to set to 1, making the rest zero. This means that without any optimizations, there are 111 choose 11 possible matrices. This is approximately 4.7×10^{14} possible incidence matrices, and that does not include time for book-keeping to make sure that cases are only checked once and to run each case through a validation algorithm which sees if the incidence matrix fulfills the requirements stated above. If one of these cases could be checked every second it would still take 1.49×10^7 years to complete the computation!

Below we transition into a discussion of a couple of the methods used to eliminate finite projective planes of some orders.

3.2.1 Using the Weight Enumerator

A property of a finite vector space over $\mathbf{F_2}$ known as the *weight enumerator* is a sum of the number of rows with each possible *weight*. The *weight* of a row is the sum of its entries.

The first major theorem to cut down on the number of cases that would need to be checked explained how the weight enumerator was uniquely determined by the number of rows with weights 12, 15, and 16.

Lam and collegues recieved considerable praise from Ryser himself for showing that no finite projective plane of order 10 could exist with any rows of weight 12.

3.2.2 Collineations

In terms of the incidence matrix definition of a finite projective plane, we notice that projective planes with rows or colums swapped are essentially the same. The equivalence of such incidence matrices are explained in terms of collineations, we are just relabelling some of the points and lines. Using this fact, Lam and his colleagues were able to make some assumptions about where 1's would be in each row saying that there had to be a row with1's positioned in that fashion.

3.2.3 Backtracking

The major algorithmic technique used in the programs looking for a finite projective plane of order 10 is called Backtracking. In this case, the algorithm tries to build up a solution until it finds that some choice it has made prevents it from doing so, at which point it back tracks to the first choice before the choice that led to a dead end. This approach is somewhat similar to the dynamic programming paradigm where solutions are computed in terms of subsolutions and promising solutions are built up until they can be shown unoptimal.

3.2.4 Data structures

As with any algorithm seeking to cut down on runtime, much of the optimization came down to the smart selection of data structures. A data structure is simply a plan for how to organize data that the program will need to access. As trivial as it may sound, smart choices of data structures can make a monumental difference in runtime. For a concrete example of how a data structure effects how long it takes to find something, compare how long it takes to find a piece of paper in a sea of papers on a messy desk, a stack of papers in alphabetical order, and files sorted in a file cabinet breaking papers up into folders inside the cabinet in some reasonable manner.

It is also important to note that no matter how smart the data structure, there is always a downside. Ironically enough, some of the data structures used in the projective plane problem were so intricate that they could not grow dynamically. This led to many errors which caused Lam and his collegues to panic. A computation would keep going after throwing a single error and only at the very end of the computation would anyone be able to see that an error had ocurred! Because of how the output was organized, finding these errors was also a fairly tedious process; this was the leading cause of a few periods of excitement before finding that there was actually an error in the computation.$

4 Closing Thoughts

Following is a discussion of some of the interesting historical points from the search for a projective plane of order 10.

4.1 Computational Power

It is funny to note how the case of finding a finite projective plane of order 10 is a good example of how quickly computers develop. The longest stretch of their computation involved waiting for 2 years (from fall 1986 to November 11 1988). During these two years, the program they developed to look for a finite projective plane of order 10 was running in the background of the CRAY-1 super computer. It is estimated that the bulk of the actual computation done only took 2000-3000 hours (which is still at least 80 days!). Unfortunately, Lam and his colleagues did not own the CRAY-1, they were renting it, and even then only got to run their program on it at one of the lowest priorities.

So why was the CRAY-1 such a huge deal? It must have been the fastest thing out there, right? On average, the CRAY-1 had a floating point performance of 136 MFLOPS. For comparison, the ATI Radeon R800 has a peak performance of 3.04 TFLOPS. That means that a consumer video card today has processing power 4 orders of magnitude greater than a super computer from the late 80s! Although not surprising to the tech savy, it is hard to understand what such massive differences in computational power mean until one has a particularly hard computation to match it against; to think that what was once a fairly occult practice of looking for exotic finite projective planes could now be carried out by anyone with a little bit of enthusiasm!

4.2 Debugging

For anyone who has spent any time programming, it is common knowledge that not only is it difficult to catch all errors right up front, but many errors are not found until the code has been used in practice for a while. In the context of proving theorems computationally, this prospect is particularly unsettling, and it did in fact affect the resolution of this problem quite substantially.

On multiple occasion Lam and his colleagues found possible sources of errors in their code or the runtime of the CRAY-1. This forced them to go back and make revisions to their code and rerun tests for months at a time.

For example, 7 days after their initial conclusion that there existed no finite projective plane of order 10, one of Lam's colleagues found an error in the execution of their code, forcing them to rethink part of the computation that they had done. A similar problem was found amid epic media response after references to their success occured in popular publications such as *The New York Times.*

After a certain point, there were still errors which they could not weed out absolutely, and they were instead forced to argue for the extremely small probability of any of the errors that could have been made rippling into an incorrect conclusion.

4.3 Final Thoughts

Does a finite projective plane of order 10 exist? Problems in discrete mathematics are often driven by the corner cases, which seem to be exactly the sorts of low-probability cases under which this proof may have holes.

Even Lam himself has said the problem needs "independent verifcation, or better still, a theoretical explanation"[LAM], but amid the wide spread acceptance of the conclusion that no finite projective plane of order 10 exists, what will encourage people to look?

Understanding the proof of the Bruck-Ryser Theorem and the computational methods employed to suggest its insufficiency are definite milestones in understanding the problem, but it seems there is still more to learn.

References

[CAM] Cameron, Peter, and Peter Cameron. *Combinatorics.* Cambridge Univ Pr, 1994. Print.

[LAM] Lam, C. W. H. "The Search for a Finite Projective Plane of Order 10." *The American Mathematical Monthly.* 98.4 (1991): 305-318. Print.