Graph Theory

Jamie Morgenstern

8/10/2007

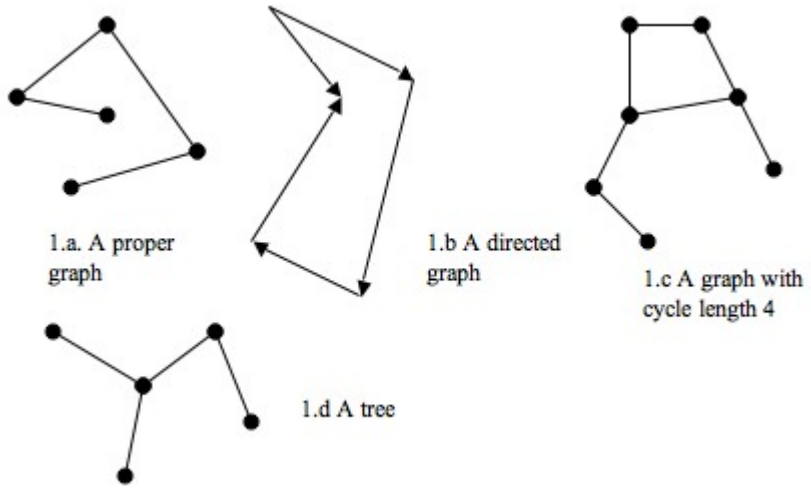
A graph is a set of nodes (points), and edges (or lines) connecting these nodes. It is often useful to refer to the size of a finite graph. The number of vertices in a graph is its order, denoted $|G|$.

Graphs may be classified in many ways apart from their order. A complete graph has each distinct pair of vertices connected by an edge. Many interesting problems arise in looking at complete graphs, several of which have to do with determining whether or not it is possible to pass through every vertex and edge once and only once (a Peterson cycle). A connected graph allows movement from any vertex to another moving along edges of the graph.

Most of the work I will be doing in this paper focuses on connected, directed graphs. Digraphs, or directed graphs, have edges that are not symmetric (if $\exists$ an edge AB from vertex A to vertex B $\nRightarrow \exists$ edge BA. Proper graphs, conversely, are not directed and edge AB is considered equivalent to edge BA. The directed edges of a digraph are called arcs.

A path is a set of vertices with edges allowing movement between the vertices. For example, if G:V=a,b,c,d,e, E=ab, bd, de, then a path is defined by ABDE. Digraphs are weakly connected if, omitting the direction of the arcs, $\exists$ a path from any vertex to any other vertex. A strongly connected digraph has a path from any vertex to any other vertex even when considering the direction of the arcs.

If a path begins and ends at the same vertex, the path is called a cycle. Cycles are both interesting and problematic in many problems in graph theory. Trees are connected graphs without cycles, and have many applications in circuitry. Here are some examples:



Now, it is time to look at the square of a directed graph. A squared graph takes the original graph, and adds an arc (ac) for each pair of arcs of the form (ab, bc).

An oriented graph is a directed graph, with no loops (an arc that begins and ends at the same vertex) or multiple edges (which allows only one direction of an arc between two vertices). The out-degree of a vertex G can be denoted deg+(G). It is important to note that the square of an oriented graph may or may not be an oriented graph; the square is a digraph and may have multiple edges.

This problem (stolen from Nate Dean, of Texas Southern University) is one I found of particular interest.

Prove that for every oriented graph, D, there exists a vertex whose out-degree at least doubles when you square the oriented graph.

For an algorithm to create this squared graph, one begins by taking a list of the vertices. For each vertex N, every out-arc (defined here as an edge beginning at N and terminating at another vertex M) from N must be listed. The out-arcs from M must then be paired with the out-arcs from N to any other vertex. Each of these distinct pairings calls for a drawing of a new out-arc from M to the end vertex of the out-arc from M. Every vertex must be examined for these "'pairings"' until a complete list is made. In the end, a list of each vertex and the corresponding paths of length two from each vertex will be made and additional arcs drawn from the first vertex to the end of second arc.

This has already been proven for tournaments. A tournament is a complete, oriented graph. Surprisingly, the proof was not available for viewing; but it

seems to me the proof would be along these lines.

Claim: For every oriented graph, D, there exists a vertex whose out-degree at least doubles when you square the oriented graph.
Proof:

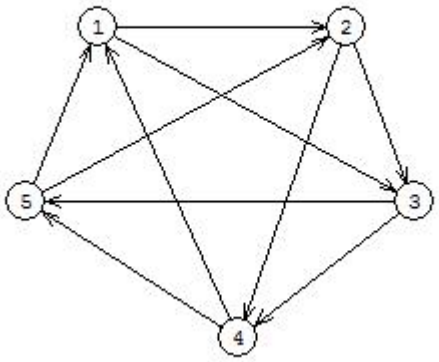
All finite oriented graphs may be separated into three cases: those with one or more vertices with an out-degree of zero, those with at least one vertex of out-degree one and all vertices having out-degree of at least one, and those with vertices all with out-degree greater than one.

Case 1: Graphs with at least one vertex B of out-degree 0 The square of this graph has vertex B with outdegree zero by the algorithm I classified above. 2*0=0, so this case is trivially true.

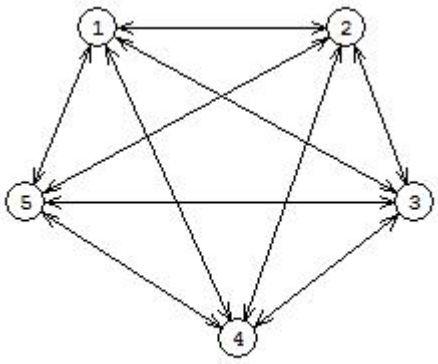
Case 2: Graphs with all vertices of outdegree at least one Consider a vertex S with an out-arc to vertex T (and only one out-arc). The vertex T must connect to another vertex (to a new vertex U) through an arc. According to our algorithm, a second out-arc(SU) will be added to the graph in squaring. Therefore, the out-degree of S has been doubled.

Case 3: Graphs with all vertices of outdegree greater than one This case is slightly more interesting than the others.

To begin, one considers vertex R, which necessarily contains at least two out-arcs, one to vertex Q and one to vertex S. Each of these, in turn, must have out-arcs. In the smallest case, these three vertices are the only three in the graph; so each vertex has a path of length one to each other vertex. But this does not satisfy one of our original conditions; we may not have arcs AB and BA in an oriented graph. So we must assume, then, that we must have at least four vertices, but this creates the same problem. An oriented graph with five vertices is the first one that allows such a construct:



This particular graph, when squared, creates the following:



For this example, it is easy enough to see that the claim holds. In fact, the out-degree of each of the vertices is doubled. For any oriented graph with out-degrees all greater than two, this also is true.

If we consider the vertex M with the minimum out-degree, it is clear that each of the other vertices must have at least that out-degree. Now, we consider the vertices M is connected to via its out-arcs. Each of these vertices must reach some "'new"' vertices(vertices that were not the original vertices considered)with their out-arcs, else there would be multiple edges between these vertices. Therefore, when the graph is squared, vertex M will have new arcs to these new vertices, and will have at least twice as many out-arcs as the original graph.

Another interesting problem was presented to me by Lazlo Babai, in his Incomplete Lecture notes on Discrete mathematics. The results of this problem relate to graph theory, though the work I have done has focused on a proof which does not use graph theory.

Let p be a prime. An integer z is a quadratic residue mod p if $z \not\equiv 0 mod p$ and $(\exists x)(x^2 \equiv z(mod p))$.

Babai's notes first suggest looking at the quadratic residues mod 5 and mod 7. In the case of mod 5, 1 and 4 are quadratic residues. This follows from $1^2 \equiv 1 \equiv 4^2 (\text{mod } 5)$ and $2^2 \equiv 4 \equiv 3^2 (\text{mod } 5)$. Mod 7 has 1, 4, and 2 for quadratic residues: $1^2 \equiv 1 \equiv 6^2 (\text{mod } 7)$, $2^2 \equiv 4 \equiv 5^2 (\text{mod } 7)$, and $3^2 \equiv 2 \equiv 4^2 (\text{mod } 7)$.

This suggests a pattern. I chose to investigate: Here is a table describing my initial findings:

p	1	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2	11^2	12^2	13^2
3	1	1											
5	1	4	4	1									
7	1	4	2	2	4	1							
11	1	4	9	5	3	3	5	9	4	1			
13	1	4	9	3	12	10	10	12	3	9	4	1	

The obvious question from here is to ask: why these pairings in quadratic residue classes? And where does it lead us? Indeed, the next exercise in Babai's ask for something of the like. His exercise asked to prove that if p is an odd prime, then the number of non-congruent quadratic residues mod p is $(p-1)/2$.

First, $\exists$ p equivalence classes mod p, and $(p-1)$ equivalence classes not equivalent to 0. The pairings suggest we look for a correlation between these equivalence classes and their squares.

If, for some $c : 1 \leq c \leq (p-1)$ $\exists b : b^2 \equiv c$, then $(p-b)^2 \equiv c$.

Proof:

$(p-b)^2$

$= p^2 - 2pb + b^2$

$\equiv b^2$ mod p

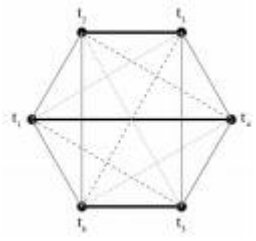
And equivalence classes are transitive. Thus, if $b^2 \equiv c$ mod p, then $(p-b)^2 \equiv b^2 \equiv c$.

This result of modular arithmetic has a very exciting result for us. The (p-1) equivalence classes mod p can each be squared, but only 1/2 of them will have distinct squares mod p. Therefore, $\exists (p-1)/2$ quadratic residues mod p.

Next, the Payley graph is defined as follows. The vertices, $V = 0, 1..(p-1)$, are connected by arcs based on quadratic residues in this way: $u \rightarrow v$ if $(u-v)$ is a quadratic residue mod p.

Several interesting exercises are recommended from here. First, let us examine the graphs created if $p \equiv -1$ (mod 4). The list of primes satisfying this condition begins with 3, 7, and 11. What do these Payley graphs look like?

The notes suggest they are tournaments. And indeed, when a graph is constructed with the above specifications, with the case p=7 as an example, we get a tournament:



For p$\equiv$1 mod 4, a graph is defined rather than a tournament(as in this case of p=5), as $4-1 \equiv 3$, $1-4 \equiv 2$ mod 5, neither of which are residues, so vertex 1 and 4 are not connected.

Now, the task is to prove this tournament occurs for every prime p$\equiv$ 3 mod 4, and does not occur for p$\equiv$ 1 mod 4, instead, in this case, we get a graph. Let us start with the case of primes $\equiv$ 1 mod 4. The key observation from Babai's notes is that -1 is a quadratic residue mod p when p $\equiv$ 1 mod 4 but not when p$\equiv$ 3 mod 4.

Claim: For any prime p $\equiv$ 3 mod 4, the graph constructed by adding an edge between vertices u and v $u, v | 0 \leq u, v \leq (p-1)$ iff u-v is a quadratic residue mod p gives a tournament.

Proof:

The claim can be restated as: in mod p (where p $\equiv$ 3 mod 4), $\nexists$ two non-residues which sum to 0 mod p. This comes from looking at $(u-v)+(v-u) = 0$, because both cases must be considered when deciding if the two vertices share an edge.

Consider some quadratic residue y. By definintion, y$\equiv$ r^2 mod p. If two quadratic residues are multiplied together, the result is a quadratic residue (z$\equiv$ t^2, $yz \equiv (rt)^2$).

But, if a quadratic residue is multiplied by a nonresidue, the result is a nonresidue. So, $-1 * y = -y$, or the additive inverse of y **(and the only distinct additive inverse of y mod p) must NOT be a quadratic residue mod p**. Therefore, for all -y, the opposite holds (namely, multiplying -y by -1 gives $-1 * -y = (-1)^2 r^2$. This is true for all quadratic residues mod p, or, to rephrase, $\forall y$, -y is a nonresidue. It follows that all nonresidues have additive inverses which are residues. Therefore, (u-v) (strictly either) or (v-u) must be a quadratic residue mod p. This creates the aforementioned tournament.

Why does the above argument fail for p$\equiv$ 1 mod 4? In this case, -1 is a quadratic residue, so $\exists$ t,-t s.t. neither are quadratic residues, leaving two vertices r and s unconnected, yielding a graph instead of a tournament.