GRT Statements
A Collection of Unsubstantiated Claims

Nick Spinale
Budapest Semesters in Mathematics
Introduction to Mathematical Cryptography

Compiled: Wednesday 12th October, 2016

Tuesday 6th September, 2016

Definition. If V is a set and $E \subseteq \binom{[V]}{2}$, then $G = \langle V, E \rangle$ is a simple graph.

Definition. H is a subgraph of a graph G if H is a graph and $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

Definition. If G is a graph and $A \subseteq V(G)$, the induced subgraph of G for vertex set A, denoted $G[A]$, is $\langle A, \{e \in E(G) : e \cap A \neq \varnothing\} \rangle$.

Definition. Graphs F and G are isomorphic iff there exists some $h : V(F) \leftrightarrow V(G)$ such that $uv \in E(F) \iff h(u)h(v) \in E(G)$.

Definition. $\langle V, E \rangle$ where $V = \binom{[5]}{2}$ and $uv \in E$ iff $u \cap v = \varnothing$ is called the Peterseu graph.

Definition. If G is a graph, then a sequence of vertices in G $x_1 x_2 \dots x_{n+1}$ such that $x_i x_{i+1} \in E(G)$ for all $1 \leq i \leq n$ is a walk.

Definition. A path is a walk with no repeated vertices.

Definition. A cycle is a walk of more than four vertices where all but the first and last are unique.

Definition. Assume G is a graph. Then the compliment of G, denoted $\bar{G}$, is $\langle V(G), \binom{V(G)}{2} \setminus E(G) \rangle$.

Definition. The degree of a vertex is the number of edges that contain it.

Definition. A graph is connected if, for any two vertices, there is a path between them.

Definition. A graph G is minimally connected if it is connected, but for all $v \in V(G)$, $G[V(G) \setminus v]$ is not connected.

Definition. A tree is a graph that is both connected and contains no cycles.

Theorem. *A tree on at least 2 vertices always contains at least 2 vertices of degree 1.*

Theorem. *A tree on n vertices has $n - 1$ edges.*

Definition. The Prüfer code is way of encoding a tree into a sequence of natural numbers. The Prüfer code of a tree on n vertices can be obtained in the following way:

1. Label the vertices $1, 2, \dots, n$.
2. Until only one vertex remains, remove the leaf with the smallest label, and append the label of its neighbor to the sequence.

Proposition. *The Prüfer code of a tree on n vertices has length $n - 1$ and ends in n. Furthermore, every sequence of $n-1$ natural numbers between 1 and n ending in n encodes exaclty one tree on n labelled vertices.*

Theorem (Cayley)**.** *There are n^{n-2} different trees on n labelled vertices.*

Thursday 8th September, 2016

Definition. An Eulerian circuit is a closed walk that contains every edge exactly once. An Eulerian path is an open walk that contains every edge exactly once.

Theorem. *A graph contains an Eulerian circuit iff it is connected and all vertices have even degree.*

Corollary. *A graph contains an Eulerian path iff it is connected and has exactly two vertices of odd degree.*

Fact. *If G is a graph, then $\Sigma_{v \in V(G)} d(v)$ is even.*

[Homework]

Proposition. *Every simple graph contains 2 vertices of even degree.*

Definition. A self-complimenting graph is isomorphic to its compliment.

Proposition. *The only two self-complimenting trees are the paths of length 2 and 4.*

Tuesday 13th September, 2016

Definition. A cycle that contains every vertex exactly once is called a Hamiltonian cycle.

Observation. If G contains a Hamiltonian cycle, then:

- G is connected.
- G has no vertices of degree 1.
- G must remain connected after the removal of any edge.
- G must remain connected after the removal of any vertex.

Fact. *If G contains a Hamiltonian cycle, then after deleting any k vertices, the resulting subgraph must have at most k connected components.*

Notation. K_n denotes the complete graph on n vertices. C_n denotes the cycle on n vertices.

Observation. Any complete graph contains a Hamiltonian cycle.

Thursday 15th September, 2016

Theorem (Dirac, 1952)**.** *If G is a graph on n vertices such that all of its vertices have degree at least $\frac{n}{2}$, then G contains a Hamiltonian cycle.*

Theorem (Ore, 1960)**.** *Assume G is a graph on n vertices. If $d(u) + d(v) \geq n$ for all $u, v \in V(G)$ such that $uv \notin E(G)$, then G contains an H-cycle.*

Theorem (Posa, 1962)**.** *Assume G is a graph on n vertices with degrees $d_1 \leq d_2 \leq d_3 \leq \cdots \leq d_n$. If $\forall k \leq \frac{n}{2} : k + 1 \leq d_k$ then G contains an H-cycle.*

Theorem (Chvátal)**.** *1. Assume G is a graph on n vertices with degrees $d_1 \leq d_2 \leq d_3 \leq \cdots \leq d_n$. G contains an H-cycle if, for all $k \leq \frac{n}{2}$ such that $d_k \leq k$, $d_{n-k} \geq n - k$.*

2. *Assume $d_1 \leq d_2 \leq d_3 \leq \cdots \leq d_n$ is a sequence of degrees and that, for some $k \leq \frac{n}{2}$, $d_k \leq k$ and $d_{n-k} \leq n - k$. There is some graph G with degrees $d'_1 \leq d'_2 \leq d'_3 \leq \cdots \leq d'_n$ such that $d'_i \geq d_i$ and G does not contain an H-cycle.*

Observation. Chvátal implies Posa, which in turn implies Dirac.

[Homework]

Notation. If G is a graph, then $\delta(G)$ is the minimum degree in G, and $\Delta(G)$ is the maximum.

Proposition. *Assume G is a graph on $2k + 1$ vertices such $\delta(G) \geq k$. G contains an H-path.*

Tuesday 20th September, 2016

Definition. Two edges are independent if they are disjoint.

Definition. A matching is a set of independent edges.

Definition. If G is a graph, then a matching containing every vertex in G (i.e. a matching of size $\frac{|V(G)|}{2}$) is called a perfect matching.

Definition. Assume G is a graph. G is called bipartite iff there exist disjoint sets A and B such that $A \cup B = V(G)$ and $\forall e \in E(G) : e \not\subseteq A \wedge e \not\subseteq B$.

Theorem. *A graph is bipartite iff it does not contain an odd cycle.*

Notation. Assume G is a graph and $X \subseteq V(G)$. $N(X) = \{v \in V(G) : \exists x \in X : xv \in E(G)\}$.

Theorem (Hall)**.** *Assume $G = \langle A, B, E\rangle$ is a bipartite graph. G contains a matching covering A iff $\forall X \subseteq A : |N(X)| \geq |X|$.*

Corollary (Frobeinus)**.** *Assume $G = \langle A, B, E\rangle$ is a bipartite graph. G contains a perfect matching iff $|A| = |B|$ and $\forall X \subseteq A : |N(X)| \geq |X|$.*

Thursday 22nd September, 2016

Theorem (Tutte)**.** *A graph G contains a perfect matching iff, for all $S \subseteq V(G)$, the number of odd components in $G[S^C]$ is less than or equal to $|S|$.*

Thursday 29th September, 2016

Definition. Let G be a graph. To each vertex in G, assign an ordering of its neighbors. This order is called a preference list. A matching is stable if there is an edge not in the matching such that each endpoint either prefers the other over its match or is unmatched. Such an edge is called an unstabilizing edge.

Theorem (Gale-Shapley)**.** *A bipartite graph always has a stable matching.*

Definition. A proper coloring of a graph G is a function $c : V(G) \to A$ such that $\forall uv \in E(G) : c(u) \neq c(v)$.

Definition. The chromatic number of a graph G, denoted $\chi(G)$, is the minimum $n \in \mathbb{N}$ such that there exists some proper coloring $c : V(G) \to [n]$.

Fact. $\chi(G) \leq \Delta(G) + 1$.

Fact. $\chi(K_n) = n$

Fact. $\chi(C_{2k+1}) = 3$

Theorem (Brooks)**.** *If G is connected and not isomorphic to the a complete graph or an odd cycle, then $\chi(G) \leq \Delta(G)$.*

Proposition. $\chi(G) \leq$ *max* $\{ \delta(H) : H$ *is an induced subgraph in* $G \} + 1$.

Definition. The clique number of G, denoted $\omega(G)$, is the size of the largest complete subgraph in G.

Proposition. $\chi(G) \geq \omega(G)$

[Homework]

Proposition. *If a graph is not bipartite, then there exists an assignment of preference lists for which no stable matching exists.*

Tuesday 4th October, 2016

Theorem. *For all $k \geq 2$, there exists some graph G such that $\chi(G) > k$ while $\omega(G) = 2$*

Definition. The girth of G, denoted $g(G)$, is the length of the shortest cycle in G.

Theorem (Erdős)**.** *For all $k \in \mathbb{N}$, there exists some graph G such that $g(G) > k$ and $\chi(G) > k$.*

Observation. There is no local reason for $\chi(G)$ to be large.

Thursday 6th October, 2016

Definition. If G is a graph, then a proper edge coloring of G is a function $c : E(G) \to A$ such that $\forall e, f \in E(G) : e \cap f \neq \varnothing \implies c(e) \neq c(f)$.

Definition. The chromatic number (or chromatic index) of the edges in a graph G, denoted $\chi_e(G)$ or $\chi'(G)$, is the least $n \in \mathbb{N}$ such that there exists a proper coloring $c : E(G) \to [n]$.

Theorem (Vizing)**.** *If G is a finite simple graph, then $\Delta(G) \geq \chi_e(G) \geq \Delta(G) + 1$.*

Observation. $\chi_e(C_{2k+1}) = \Delta(G) + 1$

Theorem (Shannon)**.** *If G is a graph (simple or otherwise), then $\chi_e(G) \leq \frac{3}{2}\Delta(G)$.*

Definition. Assume G is a graph. The line graph of G, denoted $L(G)$, is such that

- $V(L(G)) = E(G)$
- $E(L(G)) = \{\ ef : e, f \in E(G) \wedge e \cap f \neq \varnothing\ \}$

Theorem. *If G is bipartite, then $\chi(G) = \Delta(G)$.*