Editorial

Discrete Mathematics deals with objects that can assume distinct, separate values. Graph Theory, Combinatorics, Coding Theory and Cryptography are different branches of it. Various graph parameters have major role and applications in many fields such as networks, biology, chemistry, sociology, economics etc. Coding theory deals with the design of error correcting codes for the reliable transmission of information across noisy channels. Cryptography provides the foundation for information security. Public key cryptographic techniques are now in wide spread use, especially in the financial services industry, in the public sector and by individuals for their personal privacy such as E-mail. There are good research groups working in these areas in and around the city. This seminar provided these groups to mingle with the authorities in the area. The post graduate students, through the problem sessions are motivated to the world of research.

The twenty first century has witnessed an unprecedented growth in Information Technology, transmission and communication techniques. The internet and World Wide Web have become daily tools and assumes major roles in the development of science and technology. Discrete Mathematics is the key for analyzing, understanding, and developing the formal theory behind these. Recent trends in the area of Discrete Mathematics were discussed by eminent researchers in India. Also, talented young researchers presented their findings in the paper presentation session.

I must use this space to acknowledge the contributions of those who have helped us for smooth conduct of this seminar. The scholarly attributes of the academic advisor of this programme, Prof. A. Vijayakumar, Department of Mathematics, CUSAT deserve special mention. I must thank him for his consummate advice and guidance throughout the conduct of seminar and the compilation of this volume. St. Paul's College provided the venue and infrastructure. Thanks to the Manager, Principal and the Staff of this college for their support and cooperation. The contribution of the Department of Mathematics, St. Paul's College, Kalamassery was commendable. I record my sincere thanks to Ms. Valentine D'cruz, H O D and each member of the faculty and all students, especially our MSc Mathematics Students. Finally, our sincere thanks to UGC because this seminar became a reality because of the financial grant provided.

Dr. Manju K. Menon

Convenor

Contents

Chapter 1

Integer Factoring - Computational Challenges

C.E. Veni Madhavan,

Dept. of Computer Science and Automation

Indian Institute of Science, Bangalore,

Email: cevm@csa.iisc.ernet.in

In this talk the integer factoring methods are explained in detail. The main points covered are discussed here.

1.1 Primes in P and the AKS Algorithm

- n prime $\iff (x+a)^n \equiv x^n + a \bmod n, \forall a$
- n prime $\iff (x+a)^n \equiv x^n + a \bmod ((x^r-1), n) \forall a$, for appropriately chosen r
- Find least r, such that $ord_r(n) > \log^2 n$
- for $a = 1$ to $\lfloor \sqrt{\phi}(r) \log n \rfloor$ do
  if $((x+a)^n \neq x^n + a \bmod (x^r - 1, n)$. Then output the prime.

Lemma 1.1.1. *$\exists r \leqslant \max\{3, \lceil \log^5 n \rceil\}$ s.t. $ord_r(n) > \log^2 n$ Let p be a prime divisor of n, $l = \lfloor \sqrt{\phi}(r) \log n \rfloor$.*

For polynomial $f(x)$ and integer m, m is *introspective* for $f(x)$ if $(f(x))^m = f(x^m) \bmod (x^r - 1, p)$.

Lemma 1.1.2. *If m, m' are introspective numbers for $f(x)$ then so is $m.m'$. (introspective numbers are closed under multiplication)*

- m introspective for $f, g \implies m$ introspective for $f.g$

- Then the integers in the set $I = \{(n/p)^i.p^j \mid i, j \geqslant 0\}$ is introspective $\forall$ polynomials in the set $P = \{\prod_{a=0}^{l}(x+a)^{e_a} \mid e_a \geqslant 0\}$
- $G = \{I \bmod r\}$ is a subgroup of Z_r^* of size, say t
- $H = \{P \bmod (h(x), p)\}$, $h(x)$ an irreducible factor of the rth cyclotomic polynomial, is a subgroup of the multiplicative group of the finite field $F \simeq F_p[x]/(h(x))$.

Lemma 1.1.3. *AKS, H.Lenstra* $\mid H \mid \leqslant n^{\sqrt{t}}$ *if* n *is not a power of* p.

1.2 Algorithms Engineering

Typical PIV 3 GHz, linux, C Benchmarks are discussed.

- Stream Ciphers ($\simeq$1.5 Gbits/sec) :
  LFSR, non-linear FSR, FISH, PIKE, A5 ...
- Block Ciphers ($\simeq$300 Mbits/sec) :
  DES, IDEA, BLOWFISH, RC5 (64 bit); RC6, TWOFISH, MARS, RIJNDAEL, SERPENT (AES-128 bit)

- Public Key Ciphers ($\simeq$20 Kbits/sec) :

  RSA, ElGamal ($\mathbf{F}_p; \mathbf{F}_q, q = 2^n, p^n$), Elliptic Curve ($\mathbf{E}(\mathbf{F_q})$); Chor-Rivest, NTRU ...

- Digital Signatures

  (generation $\simeq$20 Kbits/sec, verification $\simeq$ 1.2 Mbits/sec) :

  RSA, ElGamal ($\mathbf{F}_p; \mathbf{F}_q, q = 2^n, p^n$), Elliptic Curve ($\mathbf{E}(\mathbf{F_q})$); blind, undeniable, group ...

- Mitsubishi Smart card M16C - 16bit, 10MHz, 64KB ROM, 4KB RAM 400 msec RSA Verification (1024 bit modulus, e = 65537)

1.3 Cryptanalysis

1. *Integer Factoring Problems (IFP)* Let N be an integer with $N = p * q$ for prime integers, p, q. Given N find the factors.

2. *Discrete Logarithm Problems (DLP)* Let G be a group. The groups to be considered are (i) the multiplicative group of the finite field $\mathbf{F}_q$, for q an odd prime or $q = 2^m$,

(ii)the additive group of points on an elliptic curve over a finite field $E(F_q)$. Let g be a fixed, distinguished element (e.g.,a generator of a cyclic group or an element of large order) of G and let $a = g^x$ for some x. Given g, a in G determine x.

3. *Statistical Analysis Problems (SAP) - cryptanalysis* Given the cipher-text $c =< c_0, \ldots, c_N >, c_j \in \{0, 1\}$ output of (i) a stream cipher or (ii) a block cipher, determine the corresponding (i) plain-text $p =< p_o, \ldots, p_N, p_j \in \{0, 1\} >$ or, (ii) symmetric key $k =< k_o, \ldots, k_n, k_j \in \{0, 1\} >$, *under various cryptanalytic scenarios* .

4. *Statistical Analysis Problems (SAP) - steganalysis* Given a *stego image* S, determine with high levels of statistical significance, (1)the presence, (ii)the length of embedded content (iii) the location of embedding and (iv) the embedded content

1.4 Integer Factoring - Basic Ideas

Factor given integer n in to its prime factors.

Special interest $n = p * q$.

1. Trial Division

   Divide n by all primes $p \leqslant \sqrt{n}$.

   Complexity: $O(n/\log n)$; exponential in $\log n$.

2. *Group Order Methods*

   based on the *smoothness* of order of a *hidden group*

   (a) $p - 1$ method

   (b) $p + 1$ method

   (c) ρ-method and λ-method

   (d) *Elliptic Curve Method* (ECM)

3. *Quadratic Congruence Methods*

   Basic idea by Fermat. Odd n can be written as $n = x^2 - y^2$.

   Solving the congruence $X^2 \equiv Y^2 \pmod{n}$ with $X \neq Y \pmod{n}$; Two factors are $\gcd(X+Y, n)$ and $\gcd(X-Y, n)$.

   (a) Dixon's Method

(b) Quadratic Sieve Method

(c) Number Field Sieve Method

1.5 Integer Factoring - Group Order Methods

$p-1$ Method by Pollard:

1. Based on Fermat's little Theorem
   $\forall p$, if $\gcd(a,p)=1$ then $a^{p-1} \equiv 1 \pmod{p}$.

2. Integer N is *B-smooth* if $p \leqslant B$ for every prime $p|N$
   e.g., 34496 is 11-smooth ($34496 = 2^6 * 7^2 * 11$).

3. Integer N is *B-power smooth* if $p^e \leqslant B$ for every prime with $p^e||N$.

4. This method succeeds if p (say) is B-power smooth.
   $\gcd(a^{B!}-1, n) = p$.
   e.g., $n = 443623$, $B = 11$, $B! = 39916800$ and $\gcd(3^{39916800}-1, n) = 617$

5. Essentially, if this method works if the subgroup $\mathbb{Z}_p^*$ contained in $\mathbb{Z}_n$ has smooth order.

$p+1$ Method:

1. Similar to $p-1$ method but succeeds if $p+1$ is smooth.
2. Much slower than $p-1$

1.6 Integer Factoring - Group Order Methods

Elliptic Curve Method: (ECM)

- An *Elliptic Curve* is a genus $g = 1$ *non-singular* curve given by

$$Y^2 = X^3 + aX + b \quad a, b \in \mathbb{F}$$

with $\Delta = -16(4a^3 + 27b^2) \neq 0$ over field $\mathbb{F}$

- Solutions of over $\mathbb{F}\times\mathbb{F}$, along with special point , forms additive abelian group; where given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, $P \neq -Q$

1. Addition: $P \neq Q$, then $P + Q = (x_3, y_3)$ where,

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2; \tag{1.1}$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_2). \tag{1.2}$$

2. Doubling: $P = Q$, then $2P = (x_3, y_3)$ where,

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1; \tag{1.3}$$

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_2). \tag{1.4}$$

- Above arithmetic is called *Chord-Tangent Law.*

- Weil-Hasse Theorem

  $p + 1 - 2\sqrt{\#\mathbb{F}} \leqslant \#(\mathbb{F}) \leqslant p + 1 + 2\sqrt{\#\mathbb{F}}$

- Define over $\mathbb{Z}_n$; doesn't form a group

- There are points P and Q such that $P + Q$ is not defined.

- Will get the factor of n when inverse doesn't exist while performing addition or doubling.

- OR factoring n succeeds if $(\mathbb{Z}_p)$ is smooth where $p|n$.
  i.e., $(B!)P =$ in $\mathbb{Z}_p$ but $(B!)P \neq$ in $\mathbb{Z}_n$
- Has lots of advantages over other methods
  - Lots of curves are available to try over $\mathbb{Z}_n$
  - Parallelization is possible
  - Many optimizations are possible for *scalar multiplication* $((B!)P)$ computation.
- Best known among group order method.
- Complexity: Sub-exponential in size of the prime factor.

1.7 Quadratic Congruence Methods : Algorithm - Dixon

1. Build the *prime base* , $P = \{p_1, \ldots, p_{\pi(v)}\}$, where $\pi(v)$ is the number of primes below v.
2. Pick a random $z, 1 \leqslant z \leqslant n-1$ and let $w = z^2 \pmod N$.
3. Factorize w over the *prime base* P. Let $w = W \times \prod p_i^{\alpha_i}$.

4. *if* $W \neq 1$, *then goto Step2 else* accumulate sufficient number (say, $\pi(v)+1$) of factorizations and store the vectors $\gamma = (\gamma_1, \ldots, \gamma_{\pi(v)+1})$ where γ represents the parity vector of the exponents, $\gamma_i \equiv \alpha_i \pmod 2$. Perform Gaussian elimination mod 2 on the parity vectors γ to get a zero vector.

5. *if* no nontrivial combination is generated in *Step4 then goto Step2 else* compute y as the product of prime powers obtained in *Step4* and let x equal the product of the corresponding z.

6. *if* $x \not\equiv \pm y \pmod N$ *then* compute $\gcd(x \pm y, N)$ and *HALT else* delete the "first w and *goto Step2*

1.8 Number Field Sieve

1. Find $a, b \in \mathcal{I}, \gcd(a,b) = 1$ such that both the rational integer $a+mb$ and the *norm* of the algebraic integer $a+\alpha b$ are *smooth* (they factorize into a small prime base).

2. Factorize the rational integer $a+mb$ as $a+mb = \prod_{p \leqslant p_{max}} p^{w_p}$,

and factorize $a + \alpha b$ into *units* and *primes* in $\mathcal{I}[\alpha]$ as

$$a + \alpha b = \prod_{u \in U} u^{t_u} \prod_{g \in G} g^{\nu_g}$$

,where $t_u \in \mathcal{I}, \nu_g \in \mathcal{I}_{\geqslant 0}$. Here U is a set of predetermined set of generators for the group of units of $\mathcal{I}[\alpha]$ and G is a set of generators for the prime ideals of prime norms $\leqslant Bound = p_{max}$. Then, since $\phi(a+b) = a+mb \pmod N$ we have the identity

$$\prod_{u \in U} \phi(u)^{t_u} \prod_{g \in G} \phi(g)^{\nu_g} \equiv \prod_{p \leqslant p_{max}} p^{w_p} \pmod N$$

3. Generate a "sufficient" number of such congruences and perform Gaussian elimination mod 2 on the exponent vectors t_u, ν_g, w_p to get nontrivial solutions to the congruence $x^2 \equiv y^2 \pmod N$ and then compute $\gcd(x \pm y, N)$.

Algorithm-NFS factors an integer N in expected time $O(\exp\{(c+ o(1))(\ln N)^{1/3}(\ln \ln N)^{2/3}\})$

Step 1 : Select an irreducible polynomial f over Q with $f(\alpha) = 0$, for $\alpha \in C$ and s.t. $\exists\ m \in Z$ with $f(m) \equiv 0 \bmod N$.

Let $K \cong Q(\alpha)$. Let $Z_K = Z[\alpha]$ be the ring of integers. Fix a factor base $\mathcal{F}$.

Step 2 : Generate a set $S = \{(c, d) \mid c, d \in Z,\ (c, d) = 1\}$ s.t., we can express

1. $c + md$ in terms of rational primes in $\mathcal{F}$
2. $c + \alpha d$ in terms of *first degree* prime ideals in $\mathcal{F}$
3. $|S|$ is greater than the size of $\mathcal{F}$

The map $\Phi : Z_K \rightarrow GF(p)$ by $\alpha \mapsto m \pmod p$ gives relations in indices of primes and first degree prime ideals.

Step 3 : Solve the linear system of equations obtained from previous step to compute the indices of rational primes and prime ideals in the factor base $\mathcal{F}$

Step 4 : Express some multiple of a in terms of *medium* size elements and compute their indices.

- Step 2 is the most time consuming, in general. It can be speeded up by selecting *good* polynomial f with *specific* properties.

- Reducing the matrix size in the Step 3
- Efficient methods for large sparse system of equations over FF.

1.9 Computational Complexity

- These heuristics have either exponential or sub-exponential time complexity in size of input ($\ln n$) given by

$$L[n, \gamma, c] = O\left(exp((c + o(1)(\ln n)^{\gamma}(\ln \ln n)^{1-\gamma}))\right),$$

  Here $1 < c \leqslant 2$ and $0 < \gamma \leqslant 1$.

- Random Squares, Quadratic Sieve : $\gamma = 1/2$. Number Field Sieve : $\gamma = 1/3$.

1.10 Our Innovations

1. *Polynomial Selection* : the low degree polynomial $f : f(m) \equiv 0 \pmod{N}$, used to specify the number field.

(coefficients, roots, large prime divisor distances)

2. *Sieving* : We are evolving, analysing and testing a variety of new heuristics to improve the practical performance.
   (multiple sieving, lattice sieving, polynomial sieving)

3. *Large systems of equations over finite fields* : The methodologies used are sparse Gaussian elimination, block Wiedemann and block Lanczos iterations.
   effect of matrix compaction effect of large prime cycles

4. setting up and solving the quadratic congruence modulo N.
   square roots of large algebraic integers

1.11 Combinatorial Problems

1. graph G on large primes in candidate relations
2. $2, 3, 4$ cycles in G
3. matchings in a bipartite version of G

4. use of information derived from items above in matrix compaction

5. densities of roots of polynomial f modulo primes in Factor Base corresponding to the first degree prime ideals

6. characterizations of number of roots in terms of coefficients of the polynomial f

1.11.1 Cryptanalysis Techniques and Effort

- Stream Ciphers :
  linear complexity profile, correlations, mul. var. poly. eqns ...

- Block Ciphers :
  differential, linear, Mod n attacks ...

- Public Key Ciphers integer factorization, discrete logarithms in groups, lattice short vectors, modular square roots ...

- side channel attacks - timing attacks, power analysis ...

- 1 Day = 86400 $>\sim 2^{16}$ seconds; 1 Year = 2^{25} seconds,

- (assuming 1 single precision int/float mul instruction = 1 cycle);

  1 MIPS/ 1 Mflops Year = 2^{45} cycles ;

  1 BIPS/ 1 Gflops Year = 2^{55} cycles ;

  1 TIPS/ 1 Tflops Year = 2^{65} cycles ;

  1 PIPS/ 1 Pflops Year = 2^{75} cycles ;

- Our PC is 1GHz Pentium IV processor = 2^{30} cycles/second ; 1 PC Year = 2^{55} cycles;

- Our super computer PARAM-PADMA delivers $\simeq 2^{40}$ cycles/second or $\simeq 2^{65} cycles/year$ - *a PARAM-PADMA year* (approximately the work-factor for factoring a 512 bit integer or *breaking* a RSA-512 key)

- DES (i) brute-force : 2^{55} trials X 2^{9} cycles per trial = 2^{64} cycles = 512 BIPS Years or = 512 PC Years

- Assuming Differential Cryptanalysis implementation with all the required storage and communication, the effort is 2^{45} trials or 2^{54} cycles or 0.5 PC Year

- Let $L(n) = \exp\{(1.93 + o(1))(\log n)^{1/3}(\log\log n)^{2/3}\}$

- $L(n)$ represents the cost of *all* computations for the currently, known, most efficient algorithms for Factoring, DL etc.

- The [1999] factoring record RSA155 (512 bit $n = pq$), would thus be $L(2^{2^9}) \sim 2^{64}$. In actual practice it was 2^{58}, that is 64 times faster than straight DES attack. I call this equivalent to 1/64 DES cracks.

- I must note that certain arithmetic ops in factoring require more cycles than DES ops. So this scaling is actually not right.

Chapter 2

Alan Turing and his Computing Legacy

C.E. Veni Madhavan,

Dept. of Computer Science and Automation

Indian Institute of Science, Bangalore,

Email: cevm@csa.iisc.ernet.in

These are the points Discussed.

2.1 Turing Points

- father - Julius Turing was in Indian Civil Service
- born: 23 June 1912 London; Sherborne School, in Dorset, 1926; King's College, Cambridge, 1931
- intellectual milieu of Russell, Whitehead and Wittgenstein - on the nature of mathematics and logic
- debates on the notion of *undecidability* of Gödel
- is there a way to identify the undecidable questions
- 1937, Turing's influential paper *On Computable Numbers*: in Turing's words, "it is about the difficulty of telling right from wrong"
- **TP 1**: postulated an abstract machine that performed an *algorithm*
- **TP 2**: a machine that could alter its internals so that it could perform all the functions of *any* Turing machine - *a universal Turing machine*
- **TP 3**: UTM can not tame undecidable questions; but gave a model for a practical computing machine

- **TP 4**: "Dip the apple in the brew, Let the sleeping death seep through"
- **TP 5**: in 1939, Govt. Code and Cypher School (GCCS) invited Turing to be a cryptanalyst at Blechley Park
- German *Enigma* attacked by Polish Rejewski was the obsession of the Blechley think-tank
- the Enigma operators duplicated the message key (say YGB) twice and encrypted (YGBYGB)
- **TP 6**: plain-text and cipher-text association study - *crib*
- *all* key-dependent permutations could be tried by changing the *plugboard* cablings and *scrambler* settings
- **TP 7**: Rejewski, Turing (and any cryptanalyst) at this point separates the compound possibilities by looking closely at the crib
- **TP 8**: Turing worked out the chains associated with Enigma settings, a guessed plain-text and the correct plain-text
- **TP 9**: Turing invented a multi-chain processing scheme to lift the information from chains, to reduce the number

of key trials; he devised an electrical circuit to neutralise the effect of the plugboard settings

- **TP 10**: he devised a system of 26 circuits and tied these with inputs to the scramblers

- **TP 11**: thus Turing's combination of combinatorial analysis, cribs, loops and electrical circuits led to the design of the cryptanalytic engine *bombe* (coined by Rejewski earlier)

- several bombes were built, by 1941, patronized by Churchill

- the motley crew at Blechley consisted of mathematicians, engineers, linguists, historians, poets, bridge/chess players and crossword solvers

- several practical heartburns - some Enigmas (Navy) had additional reflectors; plain-text was randomized; cribs were getting rare

- a final combination of, what I call *backdoors, trapdoors and side-channels*, were employed by the British to circumvent these

- Turing: computation, algorithm, language, machine, program
- Turing: efficacy and efficiency
- Turing: cryptanalysis and reversal (inversion) of computation
- AI: Turing test
- cryptanalysis - models, side channels
- machine computation and cognition
- self-reflection, introspection, free-will, extension:
- a TM with an interpretive program that analyses its own actions and predicts its future actions [Minsky, Simon]
- even such a program is NOT human - require a “heuristic” mental model and a “mentalese”

Chapter 3

An invitation to Coding Theory

C. R. Pradeep, Channabasaveshwara Institute of Technology
Gubbi, Karnataka,
Email: seearepi@gmail.com

This is a note based on which a course of two talks on Coding Theory was presented for a non-specialist diverse audience. Coding Theory, also known as Error Correcting Codes (ECC), is an important branch of mathematical theory of electrical com-

munication. As the name suggests, ECC deals with correcting the errors sent through a noisy channel. More elaborately this means, if a signal is sent and the signal gets corrupted due to the effects of the medium through which the signal travels, then the receiver gets an incorrect message. Coding theory studies ways and means of detecting and correcting such errors.

3.1 Introduction

Following is a non-mathematical illustration of this. Suppose one receives the following message

KARELA IS A BEUAFITUL STYTE

One can use ones knowledge of English language and refer to the context of the message and decode it as

KERALA IS A BEAUTIFUL STATE

The main reason for detecting and correcting the errors is the previous knowledge of English. Since both the sender and the receiver had put in efforts to learn the language they have been able to communicate in an error free fashion. Essentially Coding theory tells us how this is done between two machines. A common language and unambiguous rules need to be taught to both machines regarding spellings of the words in a message. One has to start by fixing an alphabet! Normally alphabets used in a communication system could be symbols representing elements of a finite field (or these days algebraic number fields!). But for our lectures we (mostly) stick to the binary field consisting of 0, 1. The words are fixed to be elements of particular subspaces of vector spaces over finite fields. This is how Linear Algebra plays a pivotal role in Coding Theory. In fact for a mathematician, classical coding theory is nothing bur linear algebra over finite fields. How the dimensions of the vector space and the subspace are related to number of words and distance between the words shall be explained in the talk. Distance between two words is essentially a measure of how different the

words are. These give raise to various bounds mentioned at the end of this note.

3.2 Definitions

A **q-ary linear code** C is a linear subspace of F_q^n, the n-dimensional vector space over finite field with q elements. If C has dimension k, it is called $[n, k] - code$.

The **Hamming distance** between two code words x and y is the number of coordinates in which they differ.
The $weightw(x)$ is defined as distance between x and 0. At times and $[n, k]$-code is denoted by $[n, k, d]$-code where d is the minimum of all weights in the code.

A **generator matrix** G for a $[n, k]$-code C is kn matrix whose rows are a basis of C.

If C is a [n, k]-code, the dual code $C^{\perp}$ is defined by all the

vectors in F_q^n which are orthogonal to every vector in C. Here standard inner product is to be used. If $G = [I_k P]$ is a generator matrix in the standard form of the code C, the $H = [-P^{\perp} I_{n-k}]$ is a generator matrix of $C^{\perp}$. H is also called parity check matrix of C.

3.3 Some standard codes and their properties

Hamming codes: A binary code Cm of length $n = 2m-1, m > 1$, with an $m(2m-1)$ parity-check matrix H is called a binary Hamming code if the columns of H are the binary representations of the integers $1, 2, 3, 2m-1$. This is a 1-error correcting code of dimension $(2m - m - 1)$.

Cyclic codes: Cyclic codes are a class of codes with the property that if (a_0, a_1, a_2, a_{n-1}) is a code word, then so is $(a_{n-1}, a_0, a_1, a_2, a_{n-2})$. As will be seen in the lecture, the following result will be crucial

in understanding the link between algebra and coding theory of cyclic codes. A linear code C is cyclic if and only if C is an ideal of $F_q[x]$. Since ideals in $F_q[x]$ are principal, the code may be specified by specifying the generator polynomial of the ideal or even by specifying the roots of the polynomial. This is what is exploited in the definition of BCH codes.

Let b be a nonnegative integer and let α be a primitive nth root of unity in $F_(q^m)$ where m is the multiplicative order of *qmodulon*. A BCH code over F_q of length n and designed distance $d, 2 \leqslant d \leqslant n$, is a cyclic code defined by the roots $\alpha^b, \alpha^{b+1}, \alpha^(b+2), \alpha^(b+d-2)$ of the generator polynomial. Special cases of BCH codes are very important. E.g., if $n = q-1$, a BCH code of length n over F_q is called **Reed-Solomon Codes**.

3.4 Some important bounds

- A code C with minimum distance d can correct upto t errors if $d \geqslant 2t+1$.
- **(Hamming bound)** Let C be a t-error correcting code

over F_q of length n with M code words. Then $M(1 + (n_{C1})(q-1) + (n_{C2})(q-1)^2 + ...+(n_{Ct})(q-1)^t \leqslant q^n$.

- **(Plotkin bound)** For a linear $[n, k]$-code C over F_q of distance d, we have $d \leqslant \frac{(nq^{(}(k-1))(q-1))}{(q^k-1)}$.

- **(Gilbert-Varshamov bound)** There exists a linear $[n, k]$-code C over F_q with minimum distance $\geqslant d$, whenever $q^{(}(n-k)) \geqslant \sum((n-1)_{Ci})(q-1)^i$.

Bibliography

[1] J. H. Van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, 1999.

[2] Ron M. Roth, *Introduction to Coding Theory*, Cambridge University Press, 2006.

[3] Richard E. Blahut, Algebraic codes for data transmission, Cambridge University Press, 2003.

[4] W. Cary Huffman and Vera Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.

Chapter 4

World Wide Web Graph

Ambat Vijayakumar,

Department of Mathematics

Cochin University of Science and Technology

Cochin-682 022, Kerala

Email: vambat@gmail.com.

4.1 Introduction

The topic of my talk could be called the 'Graph Theory in the Information Age' as well. Origin of Graph theory could be traced back to about two hundred eight years, when the legendary Swiss mathematician Leonhard Euler(1707-1783) presented a solution of the celebrated KONIGS BERG BRIDGES PROBLEM' on 26th August 1735 in the St.Peters academy. "The Konigsberg Bridge Problem is Euler's most famous work," though scholars in other specialties (differential equations, complex analysis, calculus of variations, combinatorics, number theory, physics, naval architecture, music, . ..) might disagree.".

Biggs, Lloyd and Wilson [ ] has remarked that "The origins of graph theory are humble, even frivolous. Whereas many branches of mathematics were motivated by fundamental problems of calculation, motion, and measurement, the problems which led to the development of graph theory were often little more than puzzles, designed to test the ingenuity rather than to stimulate the imagination. But despite the apparent triviality of such puzzles, they captured the interest of mathematicians,

with the result that graph theory has become a subject rich in theoretical results of a surprising variety and depth."

But , exciting, interdisciplinary applications of graph theory, especially for the past fifty years is remarkable, thanks to computer science. The storing of information has a long history starting from the papyrus and the printed books to the present day complex interconnected web pages. From the first ever website published in August 1991, by Tim Berners -Lee at CERN, the present number exceeds 1,000,000,000.

The world wide web graph W has as its vertices the web pages and edges corresponding to the links between these pages. W is a dynamic, sparse, self organising, small world, and power law network. The Small world network is a network in which most vertices are not neighbours of one another but most of them can be reached from every other by a small number of steps. Such networks are characterised by dense local clustering or cliquishness. It turns out that such networks are plenty , such as citation networks, electric power grids, telephone class graphs,

human brain networks, protein-protein interaction networks etc.

Collaboration graphs, in particular the research collaboration network of Paul Erdos itself is an interesting object of study. Due to its huge size , the structure of the world wide web continued to be an enigma. It was first described in [1] and also the journal, Nature (405, 2000) that W has a bow-tie structure, the knot consisting of a strongly connected component or core. We shall discuss some of these very exciting interdisciplinary aspects of the real world networks.

Bibliography

[1] A.Bonato, A course on the Web graph, AMS, Vol.89, 2008.

[2] R.Albert,H.Jeong,A.Barabasi, Diameter of the world wide web, Nature 401, 1999, 130.

[3] A.Barabasi, Linked: How everything is connected to everything else and what it means, Persus Publ. 2002.

[4] A.Broder et.al.Graph structure in the web, Computer Networks, 2000,309-320.

[5] N.L.Biggs, E.K.Lloyd, R J Wilson , Graph theory 1736-1936,Import, 1976.

[6] S.N.Dorogovtsev, J F F Mendez, Evolution of Networks, from Biological nets to the internet and WWW, OUP, 2003.

[7] D.J.Watts, Small Worlds: The Dynamics of Networks between Order and Randomness,2004.

[8] J.Guare, Six degrees of separation, Vintage, 1994.

[9] T.Luczak, R.Pralat, Protein Graphs, Internet Mathematics, 3,2006, 21-40.

Chapter 5

On strongly connected synchronizing automata

Ramesh Kumar P.,

Department of Mathematics

University of Kerala, Trivandrum, Kerala.

Email: rameshker@gmail.com

An automaton $\mathcal{A} = (Q, A, \delta)$ is a triple where Q is a finite set, called set of states, A is the input alphabet and $\delta : Q \times A \to Q$ is a function, called transition function. In order to study the

behaviour of $\mathcal{A}$ on words over A we extend δ to $Q \times A^*$ as follows:

$$\delta(q, 1) = q,$$
$$\delta(q, wa) = \delta(\delta(q, w), a),\ w \in A^*, a \in A.$$

$\mathcal{A}$ is strongly connected if for any $q, q' \in Q$ there exists a word $u \in A^*$ such that $\delta(q, u) = q'$. A word $w \in A^*$ is called synchronizing (reset) for $\mathcal{A}$ if $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. An automaton $\mathcal{A}$ is called synchronizing if it has a synchronizing word. The set of all synchronizing words of $\mathcal{A}$ ($Syn(\mathcal{A})$) is an ideal of A^*(ideal language). Here we show that $Syn(\mathcal{A})$ is a biordered set language (language accepted by a biordered set). Also every ideal regular language is the set of synchronizing words of some strongly connected automaton.

Chapter 6

On Vizing's Conjecture

Aparna Lakshmanan S.,
Department of Mathematics
St.Xavier's College for Women
Aluva - 683 101
Kerala, India
Email: aparnaren@gmail.com

The Vizing's conjecture [5], possed in 1968, is one of the famous unsolved problems in graph theory related to the domination number of the cartesian product of two graphs. The

conjecture states that, if G and H are any two graphs then $\gamma(G\Box H) \geqslant \gamma(G)\gamma(H)$. In other words, the conjecture states that the domination number is supermultiplicative with respect to cartesian product of two graphs. In this talk, we discuss some of the recent developments towards the attempts to prove or disprove the conjecture.

Keywords : Domination number, Cartesian product, Vizing's Conjecture

6.1 Basic Definitions and Terminology

We consider only finite, simple graphs $G = (V, E)$ with $|V| = n$ and $|E| = m$.

A set $S \subseteq V$ of vertices in a graph G is called a dominating set if every vertex $v \in V$ is either an element of S or is adjacent to an element of S. A dominating set S is a minimal dominating set if no proper subset of S is a dominating set. The domina-

tion number $\gamma(G)$ of a graph G is the minimum cardinality of a dominating set in G [3].

A graphical invariant σ is supermultiplicative with respect to a graph product $\times$, if given any two graphs G and H $\sigma(G\times H) \geqslant \sigma(G)\sigma(H)$ and submultiplicative if $\sigma(G \times H) \leqslant \sigma(G)\sigma(H)$. A class $\mathcal{C}$ is called a universal multiplicative class for σ on $\times$ if for every graph H, $\sigma(G \times H) = \sigma(G)\sigma(H)$ whenever $G \in \mathcal{C}$ [4].

The cartesian product of two graphs [3] $G = (V_1, E_1)$ and $H = (V_2, E_2)$, denoted by $G\Box H$ has vertex set $V_1 \times V_2$ and any two vertices (u_1, v_1) and (u_2, v_2) are adjacent in $G\Box H$ if either $u_1 = u_2$ and $v_1v_2 \in E_2$ or $u_1u_2 \in E_1$ and $v_1 = v_2$.

6.2 Vizing's Conjecture

The Vizing's conjecture [5], possed in 1968, is one of the famous unsolved problems in graph theory related to the dom-

ination number of the cartesian product of two graphs. The conjecture states that, if G and H are any two graphs then $\gamma(G\Box H) \geqslant \gamma(G)\gamma(H)$, where $G\Box H$ denotes the cartesian product of G and H. In other words, the conjecture states that the domination number is supermultiplicative with respect to cartesian product of two graphs. The conjecture is solved for special classes of graphs like those which have domination number less than or equal to three, cycles, chordal graphs etc. Interesting results were obtained on graph classes which satisfies the equality in Vizing's conjecture. A recent survey on results related to Vizing's Conjecture is [2].

6.3 Similar studies in other graph parameters and products

Vizing's Conjecture remaining unproved for decades also made the study of other graph parameters under various graph products interesting. A few examples for such parameters are independent domination number, global domination number, cographic domination number, global cographic domination num-

ber, fair domination number, chromatic number, homometric number etc. under various graph products like tensor product and strong product.

Bibliography

[1] R. Balakrishnan, K. Ranganathan, A text book of graph theory, Springer (1999).

[2] B. Brěar, P. Dorbec, W. Goddard, B. L. Hartnell, M. A. Henning, S. Klavžar, D. F. Rall, Vizing's Conjecture : a survey and recent results, J. Graph Theory, 69(1) (2012), 46 - 76.

[3] T. W. Haynes, S. T. Hedetniemi, P. J. Slater, Fundamentals of domination in graphs, Marcel Dekker, Inc. (1998).

[4] D. F. Rall, Packing and domination invariants on cartesian products and direct products, Pre-conference proceedings of International Conference on Discrete Mathematics (2006), Banglore India.

[5] V. G. Vizing, Some unsolved problems in graph theory, Uspechi Mat. Nauk 23 (1968), 6(144), 117 - 134.

Chapter 7

Brun's Theorem and Twin Prime Conjecture

K Vishnu Namboothiri,
BJM Government College, Chavara
Kollam, Kerala
Email: kvnamboothiri@gmail.com (Department of Collegiate Education, Kerala)

A technique by which the infinitude of primes was established finds the sum of harmonic series of primes. If one asks whether

this technique can be used to establish the infinitude of twin primes, the answer is NO. Brun proved that the harmonic series involving twin primes converges to a finite number. We will see a proof of this classical result.

7.1 Basic definitions and notations

Prime numbers, as all of us know, are positive integers greater than 1 with no factors other than 1 and the number itself. A composite number is a natural number greater than 1 which is not a prime. So, 1 does not belong to any of these two categories. One is just one! By *twin primes*, we mean a pair of prime numbers with difference equal to 2. For example, 3,5; 5,7; 11,13; 17,19.... There is something special about 5 above. It is the only one prime number appearing in two twin prime pairs. Why is it like that?

Lemma 7.1.1. *One of any three consecutive numbers in the AP* $2n+1$ *is a multiple of 3.*

Proof. Proof of this statement is very easy, unless you really

want to make it complicated! The three numbers are $2n+1, 2n+3, 2n+5$ and they give, *modulo* 3 the remainders 0, 1, 2 in some order. So one of them has to be a multiple of 3. □

So one of 3, 5, 7 is a multiple of 3. Here 3 itself is appearing and it is a multiple of 3, and the only prime which is a multiple of 3! But in all other cases, we are not that much fortunate. So 5 is something special; the one and only one prime in two twin prime pairs.

Now techniques like the Sieve of Eratostanes (see [3]) help us to list all primes up to a certain n. It is not very clear that whether there a sieve to list out all the twin primes. Of course the Sieve of Eratosthanes itself can be used with an extra sieving of non twin primes. But anything else more effective is there is the question.

The notion convergence of infinite series we use here is in the real analysis setting. That is, an infinite series is absolutely convergent if the sequence of partial sums of the absolute value terms converge. We will be dealing with only natural numbers and their reciprocals and so convergence and absolute convergece

mean the same for us. For a finite set A, the symbol $\#A$ denotes the number of elements in it. For an infinite set A, the symbols gives ∞. The main focus of this article is on a result related to the twin prime conjecture. We know, after Euclid, that there are infinitely many primes. The set of primes is not finite. A classic proof is available in the *Elements* of Euclid (It has been reproduced in many number theory books. Another place to find it is *Proofs from the Book* [1]). Another proof appeared from Euler later. The proof considers the infinite series of reciprocals of all the primes and proved that the sum is not finite.

$$\sum_{p \text{ a prime}} \frac{1}{p}$$

is not finite.

This implies that the collection of reciprocals cannot be finite. Can we use the same technique to show that number of twin primes is also infinite? [Twin Prime Conjecture / TPC] Set of twin primes is not finite. If we take the reciprocal sum of all twin primes and find that the sum of these reciprocals diverge, then? Since the partial sums are increasing, if it is bounded, it has to converge. So it is enough to show that it is bounded to

show that it is convergent. If it is not finite, then it is divergent. Nothing can be made out of the test then.

The roots of the twin prime conjecture cannot be easily traced out. It seems that in 1849, a French mathematician Alphonse de Polignac made the more general conjecture that For every natural number k, there are infinitely many prime pairs p and p' such that $p' - p = 2k$.

The case $k = 1$ in the above is the twin prime conjecture. For no single k, the conjecture has been verified as of today.

Coming back to our problem, if we show that the sum of reciprocals of a set of positive numbers is finite, then the number of numbers in that set has to be finite. Note that, this is not true the other way. That is, even if the sum of reciprocals is finite, it is not necessary that the number of numbers is finite. For example, the sum of reciprocals of all the squares of natural numbers is finite (and the sum if $\pi^2/6$).

An analysis of the results shows us something interesting. There are are more primes than that there are squares (since the sum of reciprocals of all natural number squares is finite).

Infact,

$$\sum_n \frac{1}{n^r}$$

taken over all natural numbers is finite when $r > 1$. So there are more primes (in some sense) than there are n^r for any $r > 1$! This also means that there are more primes than squares, making the collection of primes bigger.

Viggo Brun, a Norwegian mathematician poured water into the plan - of establishing TPC by showing that the sum of reciprocals of twin primes is infinite. In 1819, he proved that [Brun] Sum of reciprocals of twin primes is finite.

The aim of this expository article is to have a quick look at the proof of Brun. We will not elaborate the steps, but will try to comment on the important points and key ideas of his proof. The arguments are mainly combinatorial, requiring a little bit more attention. A detailed proof can be found in [2].

7.2 Sieve methods

Sieve theory is a set of general techniques in number theory, designed to count, or more realistically to estimate the size of, sifted sets of integers. (See [3] for a detailed study on sieve methods). A well known sieve is the *sieve of Eratosthenes*. It is used to find primes below a given limit by filtering non primes one bye one systematically. A key observation used in this sieve is that *every number below x which is not a prime, has a prime factor below $x^{1/2}$*. So to find all primes below 100, we need to only check whether a number N has a prime factor below 10 or not. That is, check whether 2, 3, 5, 7 are factors or not. If no is the answer for all these primes, the number taken is a prime!

$\pi(x)$ denotes the number of primes up to and including x. $\pi_2(x)$ denotes the number of twin prime pairs $(n, n+2)$ with $n \leqslant x$.

To prove the negative result (in the sense that, this discourages one from trying to prove TPC!) Brun precisely proved the following: There exists a positive constant C so that for a given

$x > 3$,

$$\pi_2(x) < C.x.\left(\frac{\log\log x}{\log x}\right)^2$$

Brun applied a a double sieving to the sequence of natural numbers so that all those numbers n were stricken out for which n or $n+2$ are composite. So, after the process, only those natural numbers n remain where $(n, n+2)$ is a prime pair.

7.3 Brun's theorem: First step

Let $T(x)$ be the number of the first members n of pairs of twin primes for which $n \leqslant x$. For example, $T(20) = \#\{3, 5, 11, 17\} = 4$. By $U(x; y)$, we mean the number of odd numbers $n \leqslant x$ for which $n(n+2)$ is not divisible by any of the odd primes $p_j \leqslant y$. For example, $U(20, 4) =$ number of odd $n \leqslant 20$ such that $n(n+2)$ not a multiple of $3 = \#\{5, 11, 17\} = 3$ Suppose now that $y \leqslant (x+2)^{1/2}$. Then if n or $n+2$ composite, it must have atleast one $p_j \leqslant y$ as factor, and so it would not be counted for finding $U(x, y)$. So, it will be removing all non prime product

$n(n+2)$.But at the same time, it might have removed $p_j(p_j+2)$ also which might have been a twin prime pair! So, if r is the number of primes $p_j \leqslant y$, then

$$T(x) \leqslant r + U(x, y) \tag{7.1}$$

Now rewrite $U(x, y)$ to find an upper bound for it. $B(x; p_1, \ldots, p_k)$ counts the number of odd numbers $n \leqslant x$ for which $n(n+2)$ is divisible by the product $p_1 \ldots p_k$ where $k \leqslant r$. That is, $B(x; p_1)$ counts the product $n(n+2)$ where n odd and p_1 divides the product. For example, $B(20; 5)$ counts the products $3.5, 5.7, 14.15, 15.17$. Using this notation, we have

$$U(x; y) = \left[\frac{x+1}{2}\right] - \sum_i B(x; p_i) + \sum_{i<j} B(x; p_i.p_j) - \sum_{i<j<k} B(x; p_i.p_j.p_k) \ldots$$

$$+(-1)^r.B(x; p_1, \ldots p_r)$$

Some sort of counting tells us why the above expression is true. By ρ^f we denote a product of f different prime factors

taken from $3, 5, \ldots, p_r$. Then

$$U(x;y) = \left[\frac{x+1}{2}\right] + \sum_{f=1}^{r}(-1)^f \sum_{\rho^f} B(x;\rho^f)$$

But calculating each and every term in the above expression RHS is as difficult as counting the twin primes itself. So at the cost of loosing the equality, we will try for an upper bound for the LHS. We will break the sum at a suitably chosen index $f = m < r$ with m even. So,

$$U(x;y) < \left[\frac{x+1}{2}\right] + \sum_{f=1}^{m}(-1)^f \sum_{\rho^f} B(x;\rho^f) \tag{7.2}$$

Now we need an alternate exrpession for $B(x;\rho^f)$.

Lemma 7.3.1. *Let ρ be an odd number and $\nu(\rho)$ the number of its different prime factors. Then the number $B(x;\rho^f)$ of odd numbers $n \leqslant x$ for which $n(n+2)$ is divisble by ρ is*

$$B(x;\rho^f) = 2^{\nu(\rho)}\left\{\frac{x}{2\rho} + \theta\right\} \text{ where } \theta \leqslant 1 \tag{7.3}$$

While prooving this result (see [2]), we see that θ is one of 0 or 1.

Clubbing expressions (7.1), (7.2), and (7.3), we get

$$T(x) \leqslant r + \frac{x}{2}\sum_{f=0}^{m}(-1)^f \sum_{\rho^{(f)}} \frac{2^f}{\rho^{(f)}} + \sum_{f=0}^{m}\sum_{\rho^{(f)}} 2^f \qquad (7.4)$$

where when $f = 0$, $\rho^0 = 1$ and $\nu(\rho^{(f)}) = f$.

7.4 Brun's theorem: Second step

Let us estimate the last term in (7.4). Since $\rho^{(f)}$ runs through all products of f prime factors, each taken from $\{3, 5, \ldots, p_r\}$, we have the last factor in the sum (7.4)

$$\sum_{f=0}^{m}\sum_{\rho^{(f)}} 2^f = \sum_{f=0}^{m}\binom{r}{f}2^f < \sum_{f=0}^{m}(2r)^f < \frac{(2r)^{m+1}}{2r-1} \leqslant (2r)^{m+1}$$

In the second sum,

$$\begin{aligned}\sum_{f=0}^{m}(-1)^f \sum_{\rho^{(f)}} \frac{2^f}{\rho^{(f)}} &= \sum_{f=0}^{r}(-1)^f \sum_{\rho^{(f)}} \frac{2^f}{\rho^{(f)}} - \sum_{f=m+1}^{r}(-1)^f \sum_{\rho^{(f)}} \frac{2^f}{\rho^{(f)}} \qquad (7.5)\\ &= \prod_{j=1}^{r}\left(1 - \frac{2}{p^j}\right) + \sum_{f=m+1}^{r}(-1)^{f-1} s_f \qquad (7.6)\end{aligned}$$

Here $s_f = \sum_{\rho^{(f)}} \frac{2^f}{\rho^{(f)}}$ is the f^{th} elementary symmetric function of the quantities $2/3, 2/5, , \ldots 2/p_r$. We finally have

$$T(x) \leqslant \frac{x}{2} \prod_{j=1}^{r} \left(1 - \frac{2}{p^j}\right) + \frac{x}{2} \sum_{f=m+1}^{r} (-1)^f s_f + (2r)^{m+1} \qquad (7.7)$$

Now

$$s_1 = \frac{2}{3} + \frac{2}{5} + \ldots + \frac{2}{p_r} = 2 \sum_{3 \leqslant p \leqslant y} \frac{1}{p}$$

. Here s_1 depends on y.

Some more computations show that

$$T(x) \leqslant y + e^{-s_1} + y^{9s_1} \qquad (7.8)$$

7.5 Brun's theorem: Third step

For y large enough, $2 \log\log y - B < s_1 < 3 \log\log y$ for a suitable positive B. Thus (7.8) becomes $T(x) \leqslant y + e^B \frac{x}{(\log y)^2} + y^{27 \log\log y}$ We will choose $y \leqslant x^{1/2}$. Put $y = x^\gamma$ where $0 < \gamma \leqslant 1/2$. Then $T(x) < x^{1/2} + e^B \frac{x}{(\gamma \log x)^2} + x^{27 \log\log x}$

A choice of $\gamma = \frac{1}{30 \log\log x}$, $x \geqslant 3$ gives finally

$$T(x) < x^{1/2} + 900 e^B x \left(\frac{\log\log x}{\log x} \right)^2 + x^{9/10} \tag{7.9}$$

Note that, for large x, the second summand will dominate the other terms. So

$$T(x) < Cx \left(\frac{\log\log x}{\log x} \right)^2 \tag{7.10}$$

for some positive C. Now connect T with the twin prime counting function to see that $\pi_2(x) \leqslant 2T(x)$ because $T(x)$ counts twin prime pairs, not twin primes. So, most of the times (!) only one twin prime is considered from such a pair.

7.6 Brun's theorem: Final step

To find the sum of reciprocals, take a partial sum,

$$S(x) = \sum_{p \text{ twin prime}, p \leqslant x} \frac{1}{p} = \sum_{3 \leqslant n \leqslant x, n \, odd} \frac{1}{n} (\pi_2(n) - \pi_2(n-2))$$

which turns out to be

$$\sum_{3\leqslant n\leqslant\infty} \frac{(\log\log n)^2}{n(\log n)^2}$$

which is convergent. This series is supposed to converge apprximately to $B = 1.902160583104$ as per computations made on twin primes found up to 1.610^15.

7.7 TPC: Current position

Though the conjecture is no way close to the conclusion, there has been some progresses. The article by K. Soundararajan ([4]) is something which everybody interested in TPC should read. The latest attempt to break TPC is the attempt after the most noted result of the decade from Y. Zhang (See [6]). He proved that, out of a certain number of numbers with difference 2, a few of them are certainly primes. After that, there has been lot more attempts by a team collaborated online under the codename *polymath* (see [5]) project. Though there has been some closer results, which improved Zhang's results, TPC cannot be said to be near the finishing point.

Bibliography

[1] Aigner, Martin; Ziegler, Gnter (2009). *Proofs from THE BOOK* (4th ed.). Berlin, New York: Springer-Verlag.

[2] Hans Rademacher, *Lectures on elementary number theory*, Blasidell Publishing Company, 1st Edition, 1964.

[3] Alina Carmen Cojocaru; M. Ram Murty (2005). An introduction to sieve methods and their applications. London Mathematical Society Student Texts 66. Cambridge University Press. pp. 80 - 112.

[4] K. Soundararajan, *Small gaps between prime numbers: the work of Goldston-Pintz-*, Bullettin of the Amer. Math. Soc, 44 (**1**) (2007) 1-18

[5] The Polymath8 Project, http://michaelnielsen.org/polymath1/index.php?title=Bounded

Chapter 8

(l, k) domination of the Mycielskian of a graph

Savitha K S,*

(Research supported by faculty development programme of UGC)

Department of Mathematics, St. Paul's College, Kalamassery-683503.

A. Vijayakumar †

Department of Mathematics, CUSAT, Cochin-682022.

*E.mail: savithaks2009@gmail.com

†E.mail:vijay@cusat.ac.in

AMS Classification: 05C69, 05C76.

Keywords: Mycielskian; (l, k) domination.

An interconnection network connects the processors of a parallel and distributed system. The topological structure of an interconnection network can be modeled by a connected graph where the vertices represent components of the network and the edges represent communication links between them. Efficiency and reliability are two important criteria in the designing of a good interconnection network. Some graph theoretic techniques that are used to study the efficiency and reliability of a network are discussed in [7, 8].

There are many network topological notions can be used to study the efficiency and reliability of a network and (l, k) domination is an important notion among them. (l, k) dominating number is used to characterize the reliability of "resources-sharing" in a network and has been recently studied in [9]. The concepts of (l, k) domination arise from the study of parallel routing fault tolerant systems. Due to wide spread demand for

reliable and efficient networks, study of this parameter becomes significant in any network system.

In a search for triangle-free graphs with arbitrarily large chromatic number, Mycielski developed an interesting graph transformation known as the *Mycielskian* of a graph [2]. For a graph $G = (V, E)$, the Mycielskian of G is the graph $\mu(G)$ with vertex set $V \cup V' \cup \{w\}$, where $V' = \{u' : u \in V\}$ and edge set $E \cup \{uv' : uv \in E\} \cup \{v'w : v' \in V'\}$. The vertex v' is called the twin of the vertex v and vice versa. The vertex w is called the root of $\mu(G)$. For $n \geqslant 2$, $\mu^n(G)$ is defined iteratively by setting $\mu^n(G) = \mu(\mu^{n-1}(G))$.

In recent times, there has been an increasing interest in the study of the Mycielskian of a graph. In[3], Fisher et al. studied the Hamiltonicity and diameter of the Mycielskian and proved that if G is hamiltonian, then so is $\mu(G)$ and diameter of $\mu(G)$= $\min(\max(2, diam(G)), 4)$. Balakrishnan and Francis Raj determined the vertex connectivity and edge connectivity of Mycielskian in [1].

Recently in [6], L.Guo et al. showed that for a connected graph G with $|V(G)| \geqslant 2$, $\mu(G)$ is super connected if and only if $\delta(G) < 2\kappa(G)$ and $\mu(G)$ is super edge connected if and only if $G \ncong K_2$. S. Francis Raj [4] investigated the vertex connectivity and edge connectivity of the generalised mycielskian of digraphs, which turned out to be a generalisation of the results due to Guo and Guo [5]. The fact that Mycielskian is an operator that produces large 'good' networks with respect to diameter and connectivity, makes it an interesting object to study the behaviour of the various topological notions .

In this paper, the (l, k) domination of the mycielskian of a graph and its iterates is studied and is observed that the mycielskian preserves reliable resource sharing, an important characteristic of a good network.

Bibliography

[6] R. Balakrishnan, S. Francis Raj, Connectivity of the Mycielskian of a graph, *Discrete Math.* **308** (2008), 2607–2610.

[2] R. Balakrishnan, K. Ranganathan, *A Textbook of Graph Theory*, 2^{nd} Edition, Springer, New York 2012.

[3] D. C. Fisher, P. A. McKenna, E. D. Boyer, Hamiltonicity, diameter, domination, packing and biclique partitions of Mycielski's graphs, *Discrete Appl. Math.* **84** (1998), 93–105.

[4] S. Francis Raj, Connectivity of the generalised Mycielskian of digraphs, *Graphs Combin.*(2012).

[5] L. Guo, X. Guo, Connevtivity of the Mycielskian of a graph, *Appl.Math.Lett* **22**(2009), 1622–1625.

[6] L. Guo, R. Liu, X. Guo, Super connectivity and Super edge connectivity of the Mycielskian of a graph, *Graphs Combin.* **28** (2012), 143–147.

[7] L. H. Hsu, C. K. Lin, *Graph Theory and Interconnection Networks*, CRC Press, Boca Raton 2009.

[8] J. M. Xu, *Topological Structure and Analysis of Interconnection Networks*, Kluwer Academic Publishers, Netherlands 2001.

[9] X. Xie, J. M. Xu, On the (l, w)- domination numbers of the circulant network, J. Combin. Math. Combin. Comput. **91** (2014), 3–18.

Chapter 9

On the Wiener Index, Wiener Polynomial and Zagreb Indices of Barbell Graph

U. Mary

Anju Antony

Department of Mathematics, Nirmala College for Women,

Coimbatore - 641 018, Tamil Nadu, India. The Wiener index is a distance-based topological index defined as half sum of the distance between all pairs of vertices in a graph. If is a subset of the vertex set of the given graph, then the Steiner distance of is defined to be the number of edges in a minimally connected sub graph of containing. The first Zagreb index is equal to the sum of the squares of the degrees of the vertices, and the second Zagreb index is equal to the sum of the products of the degrees of pairs of adjacent vertices of the underlying molecular graph. In this paper, Wiener index of Barbell graph is established. Also the First and Second Zagreb Indices of Barbell Graph are also obtained. **AMS Classification:** 05C15, 05C38,0340

Keywords: Barbell graph, Wiener polynomial, Wiener index, Zagreb Index.

9.1 Introduction

The Wiener Index is the first topological index to be used in Chemistry. It was introduced in 1947 by Harold Wiener. Wiener himself conceived W for acyclic molecules and defined it in a different manner. The definition of the Wiener Index in terms of distances between vertices of a graph was first given by Hosoya. Wiener index has many applications in Chemistry and Communication Theory. Wiener showed that the Wiener Index is closely correlated with the boiling points of Alkane molecules. In his later work, he showed that it is also correlated with other quantities including the parameters of its critical point, the density, surface tension and viscosities of its liquid phase and surface area of the molecule[1].

In his paper (Hos, 1988), Hosoya used the name Wiener polynomial while some other authors later used the name Hosoya Polynomial (Diu,2002),(Ste,2001). It is well known that the first derivative of the Hosoya Wiener Polynomial evaluated at $x = 1$ equals the Wiener Number. Higher derivatives of the Hosoya wiener polynomial have also been used as descriptors [4].

A topological index is a map from the set of chemical compounds represented by molecular graphs to the set of real numbers. Let G be a simple graph. The first Zagreb index is equal to the sum of the squares of the degrees of the vertices, and the second Zagreb index is equal to the sum of the products of the degrees of pairs of adjacent vertices of the underlying molecular graph[3].

9.2 Preliminaries

For terminology and notation in this paper, we refer to [2].

The wiener index is the first topological index to be used in Chemistry. It was introduced in 1947 by Harold Wiener. It is defined as the sum of distances between all pairs of vertices of a graph.

A topological index is a map from the set of chemical com-

pounds represented by molecular graphs to the set of real numbers. Many topological indices are closely correlated with some physico-chemical characteristics of the underlying compounds. Let G be a simple graph. The first Zagreb index $M_1(G)$ and the second Zagreb index $M_2(G)$ of G are defined in [7] respectively as

$$M_1(G) = \sum(d_i^2)$$

$$M_2(G) = \sum(d_i X d_j)$$

where d_i denotes the degree of the vertex v_i in G.

9.3 Barbell Graph

In this section, the Barbell graph and its properties are given.

A n-barbell graph is the simple graph obtained by connecting two copies of a complete graph K_n by a bridge and it is

denoted by B_p, [8].

9.3.1 Properties of Barbell Graph

1. order of $B_p = 2p$

2. size of $B_p = p(p-1)+1$

3. radius of $B_p = p$

4. diameter of $B_p = p+1$

5. eccentricity of $B_p = p+1$

9.4 Wiener Index and Wiener Polynomial of Barbell Graph

In this section, the Wiener Index and Wiener Polynomial of Barbell graph B_p for any p are computed.

Let G be the Barbell graph of order p where $p \geqslant 3$. Then the Wiener index of the barbell graph B_p is $W(B_p) = p^3 - p^2 + 4p - 3$.

The Wiener index for B_p, $p = 3, 4, 5$ can be computed as follows.

By virtue of definition of Wiener index, we get the following.

$W(B_3) = 27$

$W(B_4) = 52$

$W(B_5) = 85$

$W(B_6) = 126$

Proceeding like this, we observe that $W(B_p) = p^3 - p^2 + 4p - 3$.

The Wiener Polynomial of B_p for $p = 3, 4, 5, 6...$ is given by

$W(B_3, x) = 4x^3 + 4x^2 + 7x$

$W(B_4, x) = 9x^3 + 6x^2 + 13x$

$W(B_5, x) = 16x^3 + 8x^2 + 21x$

$W(B_6, x) = 25x^3 + 10x^2 + 31x$

Proof. For B_p, for $p = 3$, there are 7 pairs of vertices contributing distance one to the graph, 4 pairs of vertices contributing distance two to the graph and 4 pairs of vertices contributing dis-

tance three to the graph. Therefore, $W(B_3, x) = 4x^3 + 4x^2 + 7x$

For B_p, for $p = 4$, there are 13 pairs of vertices contributing distance one to the graph, 6 pairs of vertices contributing distance two to the graph and 9 pairs of vertices contributing distance three to the graph. Therefore, $W(B_4, x) = 9x^3 + 6x^2 + 13x$
For B_p, for $p = 5$, there are 21 pairs of vertices contributing distance one to the graph, 8 pairs of vertices contributing distance two to the graph and 16 pairs of vertices contributing distance three to the graph. Therefore $W(B_5, x) = 16x^3 + 8x^2 + 21x$
For , B_p, for $p = 6$ there are 31 pairs of vertices contributing distance one to the graph,10 pairs of vertices contributing distance two to the graph and 25 pairs of vertices contributing distance three to the graph. Therefore, $W(B_6, x) = 25x^3 + 10x^2 + 31x$
Similarly, a Wiener polynomial of W_p, $p > 7$ can be computed. Also it can be generalised as $W(B_p, x) = (p^2 - p - 1)x + (2p - 2)x^2 + p(p - 1)^2x^3$. □

First and Second Zagreb Indices of Barbell Graph

Proof. In this section, the First and second Zagreb Indices of

Barbell Graph B_p, for $p = 3, 4, 5, 6$ are computed. □

9.5 First Zagreb Index of Barbell Graph

Let B_p be the Barbell graph of order p, where $p \geqslant 3$ and the First Zagreb index of the Barbell graph is $M_1(B_p) = 2[(p-1)^3 + p^2]$

Proof. The First Zagreb index of B_p for $p > 3$ can be computed as follows.

By the definition of first Zagreb index, $M_1 = \sum(\delta(u_i)^2)$. For B_3, 4 vertices of B_3 have degree 2 and 2 vertices of B_3 have degree 3. For B_4, 2 vertices of have degree 3 and 2 vertices of B_4 have degree 4. For B_5, 8 vertices of B_5 have degree 4 and 2 vertices of have degree 5.

For any Barbell graph B_p, $2(p-1)$ vertices of B_p have degree $p-1$ and 2 vertices of B_p have degree p.

The First Zagreb Index of B_3, $M_1(B_3) = 34$. Therefore First Zagreb Index can be calculated for different values of p. $M_1(B_4) = 86$, $M_1(B_5) = 178$, $M_1(B_6) = 322$.

Hence $M_1(B_p) = \sum(\delta(u_i)^2) = 2[(p-1)^3 + p^2]$. □

9.6 Second Zagreb Index of Barbell Graph

Let B_p be the Barbell graph of order $p \geqslant 3$ and the Second Zagreb index of the barbell graph is $M_2(B_p) = (p^2-3p+2)[(p-1)(p-1)] + 1.p.p + (2p-2)(p-1.p)$.

Proof. The Second Zagreb index of B_p for $p \geqslant 4$ can be computed as follows.

By the definition of Second Zagreb index, $M_2 = \sum(d_i d_j)$.

The Barbell graph B_3 has 4 edges with end vertices of degree 2 and 2, then the centre edge (bridge) of B_3 has 1 edge with end vertex of degree 3 and 3, then 4 edges with end vertices of degree 2 and 3. The Barbell graph B_4 has 6 edges with end vertices of degree 3 and 3, then the centre edge (bridge) of B_4 has 1 edge with end vertex of degree 4 and 4, then 6 edges with end vertices of degree 3 and 4. The Barbell graph B_5 has 12 edges with end vertices of degree 4 and 4, then the centre edge (bridge) of B_5 has 1 edge with end vertex of degree 5 and 5, then 8 edges with end vertices of degree 3 and 4. Therefore the Barbell graph B_p, has $p^2 - 3p + 2$ edges with end vertices of degree $(p-1)$ and

then the centre edge(bridge) of B_p has 1 edge with end vertices of degree p and p, then $(2p-2)$ edges of B_p has end vertices of degree $p-1$ and p.

Therefore Second Zagreb Index can be calculated for different values of p. $M_2(B_3) = 41$, $M_2(B_4) = 142$, $M_2(B_5) = 285$. Proceeding like this, we observe that

$M_2(B_p) = (p^2 - 3p + 2)[(p-1)(p-1)] + 1.p.p + (2p-2)((p-1).p)$ □

9.7 Conclusion

The Wiener Index and Wiener Polynomial of any Barbell graph are computed in this paper. Also and the Zagreb Indices for Barbell graph B_p, $3 \leqslant p \leqslant 6$ has been computed. This work would be extended to find the other indices of Barbell graph for any $p \geqslant 3$ and the generalization could also be obtained.

Bibliography

[1] A.Ali and Walid A.M.Said, Wiener polynomial for Steiner distance of graphs, journal of Applied Science,Vol -8(2)2006: 64-71.

[2] Ali Aziz Ali and Herish Omer Abdullah, Hosoya Polynomial of Steiner Distance of complete m-partite Graphs and Straight Hexagonal Chains, journal of computer and maths,Vol 5(1) (2007).

[3] A.T Balaban A.T, Topological indices for structure-activity correlations, Topics Curr.Chem.Vol-114 1986)21-55

[4] Blaz Zmazek and Janez Zerovnik,Slovenia, The Hosoya Wiener Polynomial of Weighted Trees", Cratica Chemica

Acta,(2007)75-30.

[5] M.V.Diudea, Math.Comput.Chem,MATCH Commun 45 (2002) 109-122.

[6] H.Hosoya, Discrete Appl.Math, 19, (1988)239-257

[7] I. Gutman,Kinkar Ch, The first Zagreb index after 30 years, MATCH Commun.Math.Comput.chem.Vol-50 (2003), 83-92.

[8] D.Stevanovic, Discrete Math, 235 (2001), 237-244.