Global Journal of Science Frontier Research
Mathematics & Decision Sciences
Volume 12 Issue 4 Version 1.0 April 2012
Type : Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

On Geometric Models in Modern Computing and Networking

By J. V. Ramana Raju & T. Venkatesh
Jain University, Bangalore

Abstract – This paper discusses a few geometric models that have been of great utility in the modern technologically dominated society. Under the setting of topological manifolds the mathematical concepts underlying computer graphics have been explored. Other applications of the theory of manifolds in computer science and communication technology namely in codes, ciphers and networks are described. Using the concept of triangulations and homology we describe a discrete model concerning the networked environment.

Keywords : *Riemannian, surveillance, Parameterization, Splines, Hamming distance.*

2010 Mathematics Subject Classification : *53C15, 53C35 and 14J81*

Strictly as per the compliance and regulations of :

Notes

On Geometric Models in Modern Computing and Networking

J. V. Ramana Raju[α] & T. Venkatesh[σ]

Abstract - This paper discusses a few geometric models that have been of great utility in the modern technologically dominated society. Under the setting of topological manifolds the mathematical concepts underlying computer graphics have been explored. Other applications of the theory of manifolds in computer science and communication technology namely in codes, ciphers and networks are described. Using the concept of triangulations and homology we describe a discrete model concerning the networked environment.

Keywords : *Riemannian, surveillance, Parameterization, Splines, Hamming distance.*

I. Introduction

Geometric models have been playing a vital role in today's commercial enterprises albeit a fact quite unknown to the users of technology. These technologies have been essentially driven by the revolutions in e-commerce and internet usage. The Mathematical theory of communication which was initiated by C.E Shannon at Bell labs in the mid of 20th century can be regarded as a backbone of today's network revolution. To give a sample of the mathematical models driving our society, we have the theory of codes (both source codes as well as error correcting codes) which help achieve reliable and efficient transport of digital and analog data. Transactions have been taking place over the ATM Machines, Internet as well as swipe cards thanks to the mathematical description of money exchange. Security systems of e-commerce are basically operated by number theoretic and geometric models. Moreover the networked environment itself is topologically defined and several surveillance mechanisms are devised through combinatorial and geometric models. A global analysis of the same can be made through the theory of Riemann surfaces. Our basic structure in this paper is that of a manifold and we see several mathematical models that are currently used by industries world over to enable communication and trade. In section-I we look at the basic geometric spaces and their use in computer graphics and visualization. In Section -II we describe how transmission of huge digital data is possible in an error free manner by the use of geometric spaces. Also algebraic-geometry based ciphers have been discussed. In section-III we briefly describe the mathematical model for networking environment at a global scale. Finally in section-4 we look at quantum scale structures which are also motivated by the theory of manifolds and Hilbert spaces.

II. Geometric Spaces and Computer Graphics

Shapes that we need to convert into graphics can be perceived as a collection of curves. So naturally we are led to the definition of a manifold. For example if one

Author α : *Department of Mathematics, School of Graduate Studies, Jain University, Bangalore. E-mail : raamanraj@gmail.com*
Author σ : *Dean, School of Mathematics and Computing Sciences, RCU, Belgaum. E-mail : tmathvenky@yahoo.co.in*

revolves a unit line segment about a point then we see a unit disc formed. But the challenge to the computer graphics industry is to describe algorithms such that one constructs a required shape with a minimum amount of information to be fed to the computer. *Geometric Modeling* is the science of developing algorithms to construct geometric shapes and scenes as required by the graphics industry. One of the earliest methods developed in this direction is that of using polynomials to approximate surfaces. The basic idea here is to develop a mesh made of curves. This mesh is a discrete version of a manifold [2]. Using the so called algebraic splines a class of manifolds called cell polyhedral surfaces can be constructed. A suitable smoothing process then makes up the shape that we require. The crucial theoretical consideration here is that of parameterization of rational curves and surfaces. From a practical standpoint, parameterization requires many functions to be computed and hence it is a costly affair as far as computational complexity is concerned. Other alternatives are the implicit surface constructions and the conformal geometric algorithms [3].

a) Algorithms and Software

Warren and Moore's Algorithm based on triangulation of quadratic algebraic patches is one of the earliest algorithm being implemented on IBM 3D interactive accelerator. NURBS is an acronym for a class of algorithms that use the theory of algebraic curves and surfaces to generate computer graphics. It means non-uniform rational basis spline, which employs analytic techniques including Bezier curves. Pierre Bezier and Casteljau are the pioneers who developed mathematical models to build very flexible representations of curves and surfaces. If the surface or a scene to be created is already an algebraic manifold then it is relatively easy to build algorithms to represent the same on the computer screen However to get more realistic textures one uses softwares that generate fractal geometric sets. 'GANITH' is a software developed by Scientists at the Purdue University. The programmes written in C-language enable a wide range of computing with respect to graphics. The tasks that can be performed through GANITH include synthesis of graphics and rendering, spline generation, implicit surface generation and many kinds of animations.

b) Mathematical programming method

This method uses linear algebra and related algorithms to generate graphics. A scattered set of points, curves and derived jets are given as inputs. They are fed to the computer as a finite set of vectors. The output should ideally be a low degree algebraic surface fit through the scattered set of points, curves and derived jets with a prescribed higher order interpolation and least squares approximation. The mathematical problem to be solved can be expressed as follows:

Let X be a vector containing coefficients of an algebraic surface containing the points, curves and derived jets. Let M_I, M_A be the interpolation matrix and approximation matrix respectively. Then one needs to minimize $X^t(M^T_A, M_A X)$ subject to the constraints i) $M_I X=0$ and ii) $X^t X=0$

This linear programming problem which involves alignment of points curves and patches in a given pattern leads to a solution that is very helpful in the computer graphics industry.

III. Codes and Ciphers

In the modern era of ICT - Information and communication technology the right kind of processes are required for efficient transfer of data. The problems associated came to the fore when digital technology was in its infant stage. Mathematicians Richard

Ref.

2. J.Munkres, (1996) "Elements of Algebraic Topology", Addison Wessley.

Hamming and others began working towards a theory for reliable communication, which got fulfilled with the path breaking work of C.E.Shannon. He developed the so called "Mathematical Theory of communication" which became a foundation for a lot of future work to be done in this area.

a) Description of the Problem

When data has to travel through some medium which we shall call a channel, it is subjected to disturbances or 'Noise'. Errors may creep in at various positions of the digital data so much so that the receiver may not make any sense out of the scrambled data. Same is the case with the data/signals contained in a digital compact disc. So for reliable data communication one needs to encode the data in such a way that at the receiving end, a check can be performed to detect for errors and then correct all the errors that might have occurred. There is another type of encoding in literature namely source encoding. This is done whenever we need to achieve data compression. This is based on Shannon's theory of communication and the related Nyquist rate. Here we are only concerned with data encoding which is done for reliable transmission of data as described above.

b) The Solution

One of the popular methods to solve the above problem is to use vector spaces. Suppose one encodes all the message bits using an alphabet set say $\sum$ then this set need to have the structure of a finite field and the n-dimensional product space becomes a vector space of dimension 'n'. We fix the block size as 'n' so that the whole message is divided into blocks of size 'n'. In each block one deliberately keeps message bits of size n-k, thus making way for k positions for inserting check bits. The set of all meaningful words will be a subspace of the space $\sum^n$. Now after passing through the channel, the received word can be checked for errors by using the parity check matrix. The detection of error as well as the correction is done by making use of the concept of a distance on this space of (digital) words. The distance function called the Hamming distance is defined as follows:

$$d(\mathbf{x},\mathbf{y})=\{i:x_i\neq y_i,\ x_i,\ y_i \text{ are the } i\text{th position bits of x and y respectively}\}$$

c) Role of Geometry

Clearly the vector space structure and the parity check matrix play a central role in any such scheme of error correction. Now there are three parameters of any scheme of coding through vector spaces. The block size n, the number of check bits k and the minimum distance of the code. Here the minimum distance is defined as the smallest distance separating two meaningful words, among all the pairs of words, that is $D=\text{Min}\{d(x,y):x,y\ \epsilon\ C,\ x\neq y\}$.Now for the code to be efficient in the sense of faster implementation, the value of 'd' should be large while keeping the value of n also large. This is accomplished by considering an algebraic curve. The set of all rational functions on this curve is a certain ring of polynomials. It is in fact an integral domain and hence one can define a mapping from this ring into the vector space $\sum^n$. This mapping makes use of evaluation of the polynomials at the points of the curve. This is the precise geometric argument and the injectivity of the above map means that the image is a subspace of $\sum^n$. Thus we arrive at an efficient code. In very recent developments one uses a very special kind of manifold namely a Grassman manifold to develop efficient codes.

d) Ciphers

The elliptic curve which is topologically a torus has a very interesting algebraic structure. The points on this surface can be realized as an abelian group. This geometric object and of late its generalization namely an abelian variety are used in the theory of cryptograms. Cryptography is a science that assumes a very central role in today's world of electronic transactions, digitally signed documents, virtual conferences etc. Primarily one needs to protect messages being sent on a public network from the so called ***eavesdroppers*** or illegal snoopers. Another problem to be tackled in the e-commerce environment is the 'authentication' of messages. Let us say a bank has to release money to a vendor on behalf of a customer. Now the bank should be sure that the customer has made the transaction and the customer should not be able to fool the bank saying that he has not entered into a contract with the vendor (This property is called non-repudiation).

So a cipher (or ciphertext) is a transformed text out of the original text so that only the intended recipient can recover the original message and the sender himself cannot alter its content once having made the communication.

e) Discrete Log problem

Let G be a cyclic group of a very large order generated by an element 'a'. Let y be any random element of G. Then the discrete log problem in this setting is to find 'n' satisfying the equation $y=a^n$ .One implements public key cryptosystem by using this generic mathematically hard problem. Let „a" be a random element such that $1\leq a\leq q-1$. Now let us compute the number $h=g^a(\text{mod}p)$. The triple (p,g,h) is called a public key used by anybody who would like to encrypt and send messages digitally using this cipher scheme. Now the private key available only to the recipient is the number 'a'.

The Process: By using the public key (p,g,h) one encrypts a message m (plain text message is converted into a number say „m") by computing $r=g^k(\text{mod}p)$, $s=h^km$ (modp) . Note that here $0\leq m\leq p-1$

Now the required cipher text is c=(r,s). One can decrypt the message by using the secret key (i.e the private key „a") just by computing the value of $s.r^{-a}$

This simple analysis can be made extended to a more secure cryptosystem by making a judicial use of Geometric ***spaces***. The torus alluded to earlier in this article contains a neat algebraic structure namely that of an abelian group. The discrete log problem described in the previous paragraph can be suitably modified to make analogous computations on the so called elliptic curve. By a suitable identification one can visualize the torus as the set $E=\{(x,y): x^3+ax+b-y^2=0,a,b \in \mathbf{F}\}$ where **F** is a very large finite field. This set of points is in the algebro-geometric language is called an Elliptic curve.

Elliptic curve cryptography has been made very popular by some firms involved in digital signatures and digital copyrights. Researchers in this area are trying to use higher dimensional geometric spaces in search of better security since they need to be always smarter than the hacking communities.

IV. Networking Environment Model

a) Sensor Networks

A network that we use in the communication system is basically made up of several nodes that are interconnected by physical or abstract linkages. Signals which may be of digital or analog form are transmitted across these nodes. If we view the entire domain that is inter-networked, one can imagine a manifold underlying the entire gamut of devices. Sensors are devices that measure features of a domain and return a signal from

Notes

Notes

which information is extracted. More complex sensors involve video devices so as to extract visual, audio or textual data. While local topology is coarse in nature the continuum nature of a Riemann Surface is quite useful for a deeper understanding of the systems. The fundamental idea here is the **integration** of small networks to get a global surface. The local data is a triangulated domain. These discrete objects can be integrated to get a Riemannian surface. The emphasis on the Riemannian structure is to enable one to do a homological study and develop a suitable model. A network of sensors required for applications like global positioning systems, machine learning systems and other ad-hoc network devices consists of a simplicial complex made up of cloud points. These are essentially neighborhood systems made up of ε-balls. Let V be the set of points. In real world applications this is a finite set. However the mathematical abstraction has a provision of infinite points embedded in the Euclidean space R^n or on an oriented Riemann surface.With this convention we describe a discrete model.

b) Discrete Model

Based on local communication a class of simple sensors helps in fast and pervasive computing. The discretization of the Riemannian surface is as follows: The whole global area is covered by triangles formed by nodes. Each node broadcasts a unique ID number and it can detect any other node due to connectivity. The nodes have radially symmetric covering domains. The nodes on the boundary have designated properties so that neighboring devices can interact. The theory of simplicial complexes leads to this mathematical model on the said Riemannian surface. A theorem of Rado asserts that every orientable Riemann surface can be triangulated. On the other hand given any surface with a Riemannian metric given, one can put isothermal coordinates on the surface thus getting a conformal structure which leads to a complex manifold of dimension-1. Thus we get a Riemann surface say X. Let this surface have a triangulation Π made up of points of the set V. Now consider a graph G(V,E) where E is the set of edges occurring in the triangulation. Now select a spanning tree i.e a subgraph Γ with the same vertex set V but edges are selected such that no non-trivial closed paths (circuits) exist. This spanning tree helps us to form a fundamental polygon for Π .The following theorem [9] then enables us to construct a homology basis.

Theorem 3.2 Let D be a canonical cell decomposition of a compact orientable surface M of genus g. ≥1 with n_2 cells and n edges. Then (there exists) a canonical homology basis for M such that any curve in the basis is homotopic to an edge path D having atmost n_1-n_2 edges.

Thus using the short geodesics guaranteed by the above theorem one constructs a homology basis.

V. Microstructures 'a Futuristic Proposition'

In this concluding section we delve into a futuristic proposition. While the networking environment is inundated by mathematical modeling proceedures, we seek to view what is in store in the pipeline of research. According to Moore's law, the size of the computing structures is decreasing at a rapid pace. So it is worthwhile to look at the kind of innovations taking place to reduce the size of the devices (nodes) themselves. Quantum computing is the buzzword in this direction, ever since Peter Shor demonstrated the power of this kind of computing. Here the fundamentals of quantum mechanics take over the semiconductor devices to perform computing. As all of us know a computing device is a finite state machine that takes as input a string of states and after processing in finite time a desired output is generated. While these states are processed as LOGIC gates

operated by semiconductor chips, one is constantly looking for "lighter materials" in place of the bulkier ones. Thus nanotechnological advances are fast making inroads to develop miniature designs. If one uses principles of particle physics, then we lead to quantum particles and strings. Quantum computing is evolving by looking at energy states that are actually at the level of quantum packets. Non-zero equivalence classes of a Hilbert space represent all the energy states of a quantum particle. The theory of Riemann surfaces surprisingly is the right kind of mathematical abstraction to understand computing at this level. The Transition from Classical (Physics) to the Quantum setting as per Edward Witten , the Fields medalist , is very closely connected to the passage from Riemannian Geometry to Symplectic Geometry. Physicists discuss deformations mainly to look at one "The Quantum Theory" and the other to string Theory (Membranes). Symplectic Geometry was first explored because the classical equations of motions can be put in 'Hamiltonian form' and thereby symplectic properties can be utilized to solve these equations in certain important cases. Superdense coding is possible in this setting due to which in future the computing capabilities can become extremely fast almost comparable to the speed of light.

Notes

References Références Referencias

1. W.Boothby, (2002) "Introduction to Differentiable Manifolds and Riemannian Geometry", Academic Press.
2. J.Munkres, (1996) "Elements of Algebraic Topology", Addison Wessley.
3. X.Gu, Y.Wang, S.T.Yau, (2003) "Multiresolution computation of conformal structures", Systems Cybernetics and Informatics, Vol-I, Number 5.
4. Carrol.S, (2003) 'Space-Time and Geometry, an Introduction to General Relativity', Pearson Education
5. C.L.Bajaj,(1990) "Unifying Parametric and Implicit Surface Representations for Computer Graphics: Parametric Surface Display and Algebraic Surface fitting", Computer Science Technical Reports, Purdue University.
6. J.Pan, Y. T.Hon, Lin .Cai, Yi.Shi and S.X.Shen, (2003) "Topology Control for Wireless Sensor Networks, Mobi Com-03, ACM Proceedings-1
7. D.Estrin, D.Culler, K.Pister, G.Sukhatone, (2002) "Connecting the Physical World with Pervasive networks" IEEE Pervasive Computing.
8. Van de Silva, Robert Ghrist, (2007) "Homological Sensor Networks" Notices of American Mathematical Society, Vol 54, #1.
9. M.Seppala, P.Buser, (2003) "Triangulations and Homology of Riemann Surfaces" Proceeding of AMS, 13, Pp 425-432.