

DIGITAL SIGNATURE USING BÉZIER CURVES

Student Authors: Castilan, Mark Gabriel D.; Damask, Meredith Kay R.; De Leon, Deonard P.; Fabreag, Melody R.; Grapani, Julie Ann M.; Ibasco, Paul John Q.; Navarro, Cecilia M.; Naanod, Gene Reiz K.; Vega, Ginalyn V.

Adviser: Rabajante, Jomar F. e-mail: jfr_jomar@yahoo.com

**Mathematics Division, Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños**

ABSTRACT

In this generation, authentication of individual's identity is acknowledged through their facial contours, fingerprints, eye scans, and handwritings, specifically, signatures. Technological advances bring a more computer-based environment, making most registration processes and official transactions that require verification of an identity use digital marks or signatures. In this study, signatures of the authors were generated using parametric equations established by Bézier curves.

Generation of Bézier curves requires the use of Bernstein basis polynomials, $B_{i,n}(t) = \binom{n}{i} t^i (1-t)^{n-i}$. A set of initial data points, called control points, which will describe the behavior of the curve to be traced, are transformed into parametric polynomial equations. These equations are polynomials with coefficients coming from the Pascal's triangle. The derived parametric equations generate the set of x values and y values that would trace the desired curve. All computations and plotting of points can be carried-out by using spreadsheets such as MS Excel.

The process of creating digital signatures using Bézier curves is more than just creating digital signatures. This process can also be used as a fun classroom activity in teaching mathematical concepts such as polynomials, Pascal's triangle and combinations, as well as the Cartesian coordinate system.

INTRODUCTION

Simple continuous curves can be approximated using polynomials for easy analysis and evaluation. These simple curves can be combined to closely approximate a more complicated set of curves.

In Numerical Analysis, a method of generating a polynomial that passes through a given set of data points is called polynomial interpolation. A special type of polynomial called Bernstein polynomial, developed by Sergei Bernstein, was used to prove a fundamental result in approximation theory which is the Weierstrass' approximation theorem (Chabert et al 2010).

From Bernstein polynomials, a special case of polynomials can be derived. These polynomials are known as Bézier curves, named after Pierre Bézier who publicized it. Bézier curves were originally used in designing automobiles. These curves gained its reputation in computer vector graphics and animation (Choi et al 2010). Moreover, according to Casselman (2010), one of the most common uses of these curves is in font designing. Quadratic Bézier curves are used in True Type fonts (TFF); while cubic Bézier curves are used in Type 1 and TEX fonts.

In this study, the authors will focus on generating their own signatures using Bézier curves without using expensive software and advanced technical programming skills. The process only requires a spreadsheet application, and the knowledge on Cartesian coordinates, polynomials and Pascal's triangle.

METHODOLOGY

Bézier Curve is derived from Bernstein Polynomials. Suppose the following is the given set of control points ($i = 0, 1, \dots, n$):

$$p_i = \begin{bmatrix} x_i \\ y_i \end{bmatrix}$$

These points can be written in parametric form as

$$P(t) = \begin{bmatrix} x(t) \\ y(t) \end{bmatrix} = \sum_{i=0}^n \binom{n}{i} (1-t)^{n-i} t^i p_i, \quad 0 \leq t \leq 1$$

where $n + 1$ is the number of control points. The value of t should be between 0 and 1, since Bernstein polynomials uniformly converge to the desired curve only within this interval. Notice that if $t = 0$, the polynomial produces (x_0, y_0) . If $t = 1$, the polynomial produces (x_n, y_n) . As t takes on values between 0 and 1, a curve is traced but may not pass through the central points.

The following are the general steps:

Plot the control points. Using a spreadsheet, manually and creatively plot the control points (x_i, y_i) that would approximate the lines or curves of the desired graph, which in this case are the signatures.

Partition the graph to be approximated. If the graph is complex and isolated, partitioning would be necessary. For easy computation, set the maximum degree of each partition to at most 10^{th} degree. Partitions do not necessarily have the same number of points. Even though Bézier Curves are viewed as less complicated to be used than other techniques, partitioning is still required to narrow down the labor of setting degrees, substitutions and computations. Each partition will have its own parametric equation.

Determine the parametric equations. Given the different control points, determine the parametric equations per partition using the Bernstein polynomials.

Decide for the step-size of t , $t \in [0, 1]$. Consider a small value for the step size for a smoother curve, say 0.001. When the curve is too intricate, smaller step-size would give better approximations.

Evaluate the parametric equations at t , $t \in [0, 1]$. Use a spreadsheet when performing this task. Values obtained after substitution to $x(t)$ and $y(t)$ are the coordinates of the Bézier curve.

Graph the Bezier curve. In the spreadsheet, graph the generated coordinates from the different parametric equations in a single chart.

Adjust the control points when necessary. Plotting $x(t)$ and $y(t)$ may create a distorted replica of the desired graph. The control points must be adjusted for smoother curves, making the graph as close as the signature being approximated. If needed, remove or add new control points.

RESULTS

There are nine Bézier curves obtained in this paper and each represents the signature of the authors. The Bézier curve representation of these signatures are done independently for the authors to freely use their preferred number of partitions, control points for each partition and step-size for t .

The following figures are the Bézier curve representation of each of the author's signature. One of the nine signatures, which will be shown in the next section for a detailed discussion, is altered to sustain security purposes. All are plotted in MS Excel where the control points that would roughly approximate each signature are manually determined. The parametric equations that define each signature are also presented. However, only three pairs of equations are chosen to assure the security of each signature.

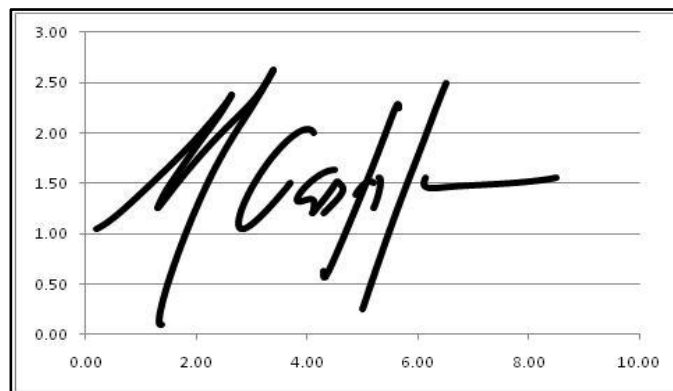


Figure 1. MGD Castilan's signature

Selected equations approximating MGD Castilan's signature:

$$x(t) = 19.47t^9 - 100.26t^8 + 195.84t^7 - 196.56t^6 + 118.44t^5 - 50.4t^4 + 16.8t^3 - 3.6t^2 + 2.7t + 0.2$$

$$y(t) = 14.35t^9 - 66.06t^8 + 115.56t^7 - 99.12t^6 + 44.1t^5 - 8.82t^4 - 0.84t^3 + 1.44t^2 + 0.72t + 1.05$$

$$x(t) = -7.06t^9 + 25.2t^8 - 40.68t^7 + 44.52t^6 - 35.28t^5 + 16.38t^4 - 2.52t^3 - 0.72t^2 - 1.17t + 2.63$$

$$y(t) = -1.79t^9 + 3.15t^8 + 6.12t^7 - 22.68t^6 + 27.72t^5 - 17.64t^4 + 5.88t^3 - 0.72t^2 - 1.17t + 2.38$$

$$x(t) = 2.89t^9 - 11.97t^8 + 47.34t^7 - 112.98t^6 + 138.6t^5 - 88.2t^4 + 27.3t^3 - 2.7t^2 + 1.8t + 1.3$$

$$y(t) = 2.535t^9 - 19.17t^8 + 59.94t^7 - 98.28t^6 + 91.35t^5 - 46.62t^4 + 10.5t^3 + 1.125t + 1.25$$

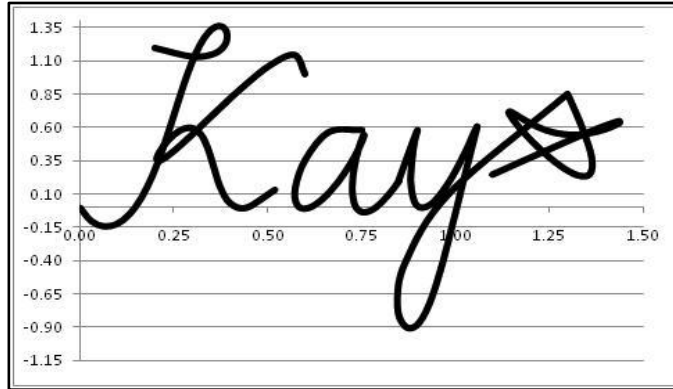


Figure 2. MKR Damask's signature

Selected equations approximating MKR Damask's signature:

$$x(t) = 5.8t^5 - 17.5t^4 + 20.0t^3 - 11.0t^2 + 2.5t + 0.2$$

$$y(t) = -25.2t^5 + 79.5t^4 - 81.0t^3 + 28.0t^2 - 2.5t + 1.2$$

$$x(t) = -5.72t^6 + 33.42t^5 - 60.72t^4 + 46.14t^3 - 13.2t^2 + 0.6$$

$$y(t) = -25.17t^6 + 163.8t^5 - 306.0t^4 + 234.0t^3 - 73.5t^2 + 6.0t + 1.0$$

$$x(t) = -15.68t^8 + 95.04t^7 - 240.24t^6 + 308.56t^5 - 202.3t^4 + 57.12t^3 - 0.56t^2 - 1.84t + 0.75$$

$$y(t) = -12.82t^8 + 129.76t^7 - 571.76t^6 + 1126.7t^5 - 1079.4t^4 + 499.52t^3 - 95.76t^2 + 3.36t + 0.58$$



Figure 3. DP de Leon's signature

Selected equations approximating DP de Leon's signature:

$$x(t) = 0.05t^5 - 0.5t^4 + 0.5t^3 - 2.0t^2 + 3.0t + 3.2$$

$$y(t) = 0.5t^5 - 1.5t^4 + t^2 + t + 3.4$$

$$x(t) = -0.2t^5 + 0.5t^4 - 1.5t^3 + 2.5t^2 - 2.25t + 4.25$$

$$y(t) = 0.25t^5 - 1.25t^4 + t^3 - 1.5t + 4.4$$

$$x(t) = -0.1t^4 - 0.4t^3 + 0.3t^2 - 1.0t + 3.3$$

$$y(t) = 0.2t^5 - 1.0t^3 + 2.0t^2 - 3.0t + 2.9$$

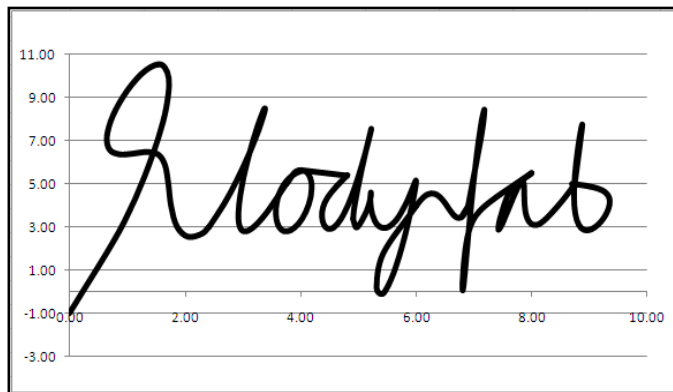


Figure 4. MR Fabreag's signature

Selected equations approximating MR Fabreag's signature:

$$x(t) = t(741.0t^8 - 3458.7t^7 + 5871.6t^6 - 4074.0t^5 + 378.0t^4 + 806.4t^3 - 226.8t^2 - 57.6t + 22.5)$$

$$y(t) = 49t^9 - 1908t^8 + 3420t^7 + 2604t^6 - 10710t^5 + 9576t^4 - 3360t^3 + 252t^2 + 81t - 1$$

$$x(t) = -1.65t^5 + 12.5t^4 - 9.0t^3 - 6.0t^2 + 5.5t + 2.4$$

$$y(t) = -19t^5 + 137t^4 - 166t^3 + 30t^2 + 20t + 3$$

$$x(t) = 610.05t^9 - 2053.4t^8 + 2462.4t^7 - 835.8t^6 - 787.5t^5 + 894.6t^4 - 327.6t^3 + 36.0t^2 + 2.25t + 3.75$$

$$y(t) = -465.2t^9 + 2754.0t^8 - 7095.6t^7 + 9987.6t^6 - 7925.4t^5 + 3213.0t^4 - 378.0t^3 - 108.0t^2 + 18.0t + 5.0$$

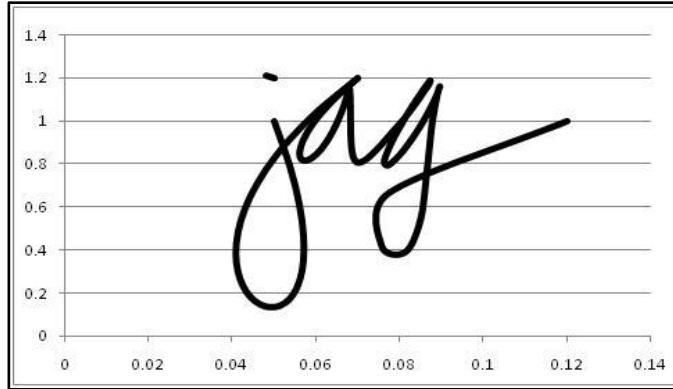


Figure 5. JAM Grapani's signature

Selected equations approximating JAM Grapani's signature:

$$x(t) = 0.257t^3 - 0.327t^2 + 0.09t + 0.05$$

$$y(t) = -1.9t^3 + 6.6t^2 - 4.5t + 1.0$$

$$x(t) = 0.05 - 0.002t$$

$$y(t) = 0.01t + 1.2$$

$$x(t) = -0.047t^3 + 0.12t^2 - 0.075t + 0.07$$

$$y(t) = 0.55t^3 + 0.6t^2 - 1.2t + 1.2$$

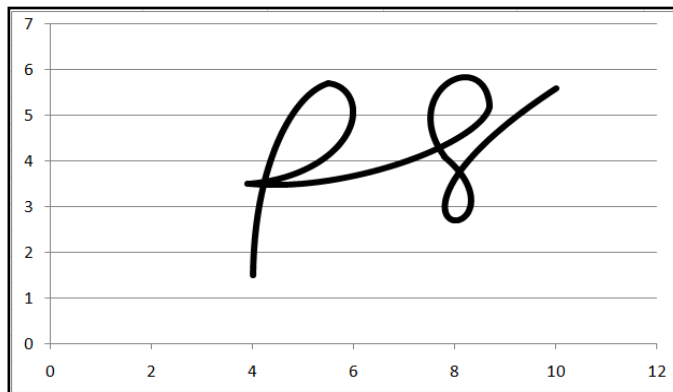


Figure 6. PJQ Ibasco's signature

Selected equations approximating PJQ Ibasco's signature:

$$x(t) = 0.05t^5 - 0.7t^4 + 1.3t^3 + 0.8t^2 + 0.05t + 4.0$$

$$y(t) = -0.3t^5 - 2.0t^3 + 2.0t^2 + 4.5t + 1.5$$

$$x(t) = -0.1t^5 + 2.0t^4 - 4.0t^3 - 2.0t^2 + 2.5t + 5.5$$

$$y(t) = 0.05t^5 - 0.5t^4 + 4.5t^3 - 6.0t^2 - 0.25t + 5.7$$

$$x(t) = 1.8t^5 - 5.5t^4 + t^3 + 3.0t^2 + 4.5t + 3.9$$

$$y(t) = 0.2t^5 - 2.0t^4 + 2.0t^3 + 2.0t^2 - 0.5t + 3.5$$

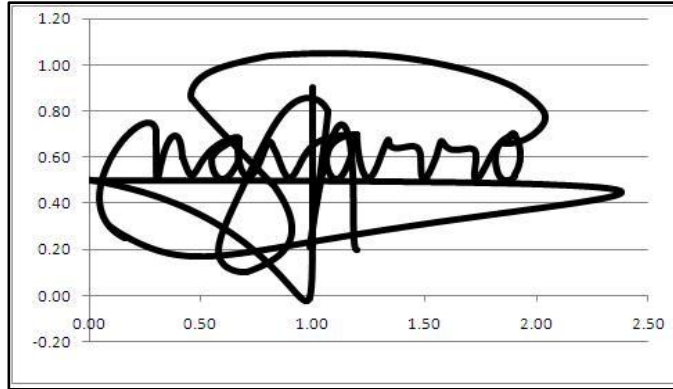


Figure 7. CM Navarro's signature

Selected equations approximating CM Navarro's signature:

$$x(t) = -1.92t^8 + 6.72t^7 - 10.92t^6 + 10.64t^5 - 6.3t^4 + 1.12t^3 + 1.68t^2 - 0.88t + 0.16$$

$$y(t) = -0.85t^8 + 1.6t^7 - 2.8t^5 + 3.5t^4 - 2.8t^3 + 1.4t^2 + 0.4t + 0.25$$

$$x(t) = 1.2t^8 - 3.6t^7 + 4.48t^6 - 3.36t^5 + 1.4t^4 + 0.3$$

$$y(t) = -1.4t^8 + 16.8t^7 - 58.8t^6 + 98.0t^5 - 87.5t^4 + 39.2t^3 - 5.6t^2 - 0.8t + 0.7$$

$$x(t) = 4.33t^8 - 6.4t^7 + 1.96t^6 - 3.92t^5 + 5.6t^4 - 1.68t^3 + 0.24t + 0.42$$

$$y(t) = -1.56t^8 + 13.12t^7 - 42.56t^6 + 67.2t^5 - 54.6t^4 + 20.16t^3 - 1.12t^2 - 0.64t + 0.6$$

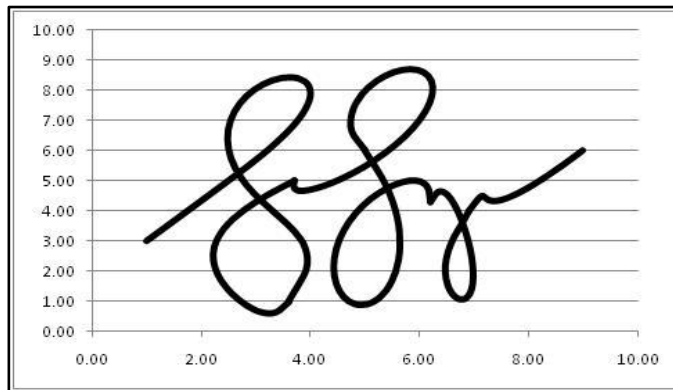


Figure 8. GV Vega's signature

Selected equations approximating GV Vega's signature:

$$x(t) = -123.6t^8 + 264.4t^7 + 100.8t^6 - 770.0t^5 + 805.0t^4 - 274.4t^3 - 25.2t^2 + 25.6t + 1.0$$

$$y(t) = -278.6t^8 + 1269.6t^7 - 2422.0t^6 + 2380.0t^5 - 1225.0t^4 + 336.0t^3 - 98.0t^2 + 36.0t + 3.0$$

$$x(t) = 108.5t^8 - 548.8t^7 + 1097.6t^6 - 1069.6t^5 + 490.0t^4 - 72.8t^3 - 4.8t + 3.6$$

$$y(t) = 1.6t^8 - 64.0t^7 + 266.0t^6 - 481.6t^5 + 490.0t^4 - 308.0t^3 + 112.0t^2 - 12.0t + 1.0$$

$$x(t) = 244.7t^8 - 1028.0t^7 + 1668.8t^6 - 1243.2t^5 + 385.0t^4 - 39.2t^3 + 14.0t^2 - 0.8t + 3.7$$

$$y(t) = -12.0t^8 - 136.8t^7 + 607.6t^6 - 840.0t^5 + 469.0t^4 - 112.0t^3 + 30.8t^2 - 5.6t + 5.0$$

I. Properties of the signatures

	Number of control points	Number of partitions	Step size	Highest degree	Lowest degree
<i>Castilan</i>	104	12	0.005	9	3
<i>Damask</i>	39	5	0.05	9	5
<i>De Leon</i>	49	10	0.005	5	1
<i>Fabreag</i>	68	9	0.05	9	3
<i>Grapani</i>	19	4	0.05	10	1
<i>Ibasco</i>	26	5	0.005	5	5
<i>Naanod</i>	32	5	0.005	10	1
<i>Navarro</i>	188	23	0.005	8	8
<i>Vega</i>	44	6	0.05	8	3

**Naanod* – refer to Discussion

Table 1 gives the number of control points, number of partitions, step size for t_i 's, and the highest and lowest degrees of the parametric equations used in generating the Bézier curve of the signatures in Figures 1 – 8.

DISCUSSION

The figure below is a sample signature and the focus of the discussion.

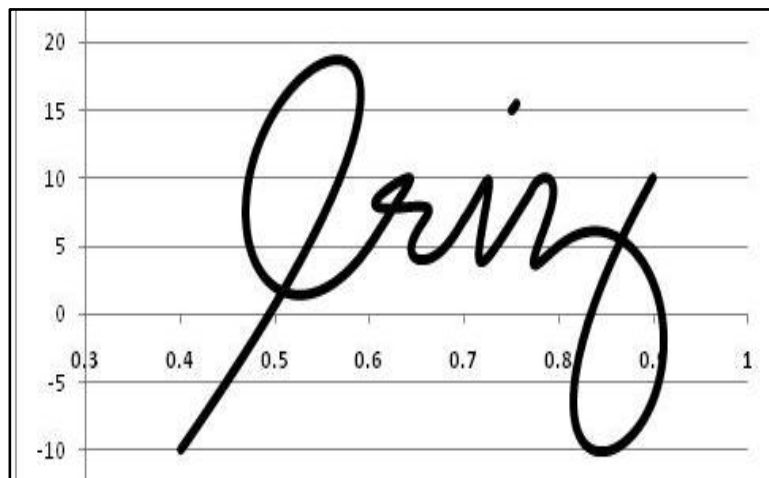


Figure 9: GRK Naanod's pseudo-signature

Figure 9 is partitioned into five. Each partition is distinguished by the letters and a symbol formed — “e”, “r”, “i”, “z” and “.”.

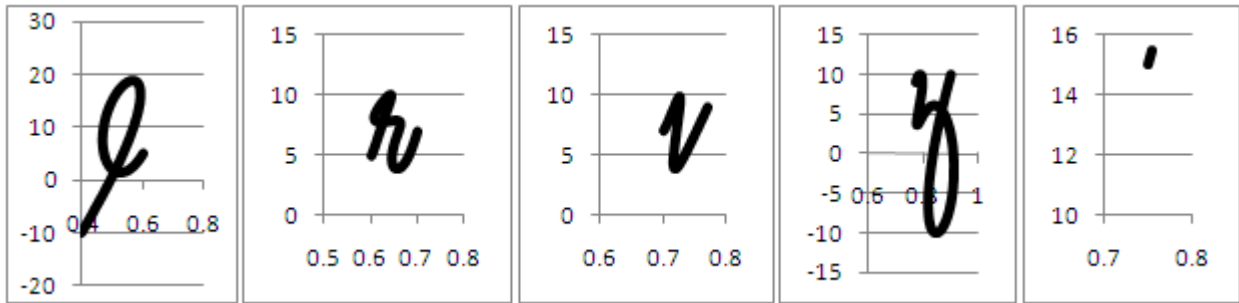


Figure 10. Partitions of the sample signature

Each partition of the sample signature has 6, 11, 6, 10 and 2 control points, respectively. The number of points for each partition was strategically chosen in a way that complicated parts of the signature are divided.

Notice that in Figure 9, the graph of the “e” partition is connected to the graph of the “r” partition. This means that the endpoint of the “e” partition is the same as the initial point of the “r” partition. Moreover, the graph of the “r” partition is connected to the graph of the “i” partition, and the “i” partition is connected to the “z” partition. However, the “.” partition is not connected to any of the previous partitions mentioned which means that it is an isolated part of the graph. With this, the total number of points that approximates the sample signature is only 32, disregarding the three repeated points. Hence, the parametric equations for the 5 partitions are of 5th, 10th, 5th, 9th and 1st degree respectively.

The control points used in generating the Bézier curve corresponding to the sample signature are given in Table 2.

II. Control points used in generating the sample signature

e		r		i		z		.	
x	y	x	y	x	y	x	y	x	y
0.40	-10.00	0.60	5.00	0.70	7.00	0.77	9.00	0.75	15.00
0.70	20.00	0.65	10.00	0.73	10.00	0.80	14.00	0.76	15.50
0.70	30.00	0.65	15.00	0.75	16.00	0.90	2.00		
0.30	20.00	0.85	10.00	0.70	0.40	0.50	5.00		
0.45	-10.00	0.00	-2.00	0.69	0.00	1.00	-13.00		
0.60	5.00	1.00	10.00	0.77	9.00	0.72	20.00		
		0.80	15.00			0.65	17.00		
		0.50	5.00			1.50	4.40		
		0.65	4.00			0.50	-40.00		
		0.65	0.80			0.90	10.00		
		0.70	7.00						

As for the parametric equations representing the signature, each control point (x_i, y_i) were substituted to $\begin{bmatrix} x(t) \\ y(t) \end{bmatrix} = \sum_{i=0}^n \binom{n}{i} (1-t)^{n-i} t^i \begin{bmatrix} x_i \\ y_i \end{bmatrix}, 0 \leq t \leq 1$. This equation is simple, making it easy to understand and manipulate whenever changes are made. The parametric equations are plotted in MS Excel using step size of 0.005. The following are the parametric equations of each of the partitions.

For “e”:

$$\begin{aligned} x(t) &= 0.4(1-t)^5 + 3.5t(1-t)^4 + 7t^2(1-t)^3 + 3t^3(1-t)^2 + 2.25t^4(1-t) \\ &\quad + 0.6t^5 \\ y(t) &= -10(1-t)^5 + 100t(1-t)^4 + 300t^2(1-t)^3 + 200t^3(1-t)^2 - 50t^4(1-t) \\ &\quad + 5t^5 \end{aligned}$$

For “r”:

$$\begin{aligned} x(t) &= 0.6(1-t)^{10} + 6.5t(1-t)^9 + 29.25t^2(1-t)^8 + 102t^3(1-t)^7 \\ &\quad + 252t^5(1-t)^5 + 168t^6(1-t)^4 + 60t^7(1-t)^3 + 29.25t^8(1-t)^2 \\ &\quad + 6.5t^9(1-t) + 0.7t^{10} \\ y(t) &= 5(1-t)^{10} + 100t(1-t)^9 + 675t^2(1-t)^8 + 1200t^3(1-t)^7 - 420t^4(1-t)^6 \\ &\quad + 2520t^5(1-t)^5 + 3150t^6(1-t)^4 + 600t^7(1-t)^3 + 180t^8(1-t)^2 \\ &\quad + 8t^9(1-t) + 7t^{10} \end{aligned}$$

For “i”:

$$\begin{aligned} x(t) &= 0.7(1-t)^5 + 3.65t(1-t)^4 + 7.5t^2(1-t)^3 + 7t^3(1-t)^2 + 3.45t^4(1-t) \\ &\quad + 0.77t^5 \\ y(t) &= 7(1-t)^5 + 50t(1-t)^4 + 160t^2(1-t)^3 + 4t^3(1-t)^2 + 9t^5 \end{aligned}$$

For “z”:

$$\begin{aligned} x(t) &= 0.77(1-t)^9 + 7.2t(1-t)^8 + 32.4t^2(1-t)^7 + 42t^3(1-t)^6 + 126t^4(1-t)^5 \\ &\quad + 90.72t^5(1-t)^4 + 54.6t^6(1-t)^3 + 54t^7(1-t)^2 + 4.5t^8(1-t) \\ &\quad + 0.9t^9 \\ y(t) &= 9(1-t)^9 + 126t(1-t)^8 + 72t^2(1-t)^7 + 420t^3(1-t)^6 - 1638t^4(1-t)^5 \\ &\quad + 2520t^5(1-t)^4 + 1428t^6(1-t)^3 + 158.40t^7(1-t)^2 - 360t^8(1-t) \\ &\quad + 10t^9 \end{aligned}$$

For “.”:

$$\begin{aligned} x(t) &= 0.75(1-t) + 0.755t \\ y(t) &= 15(1-t) + 15.5t \end{aligned}$$

The observations of the authors during the conduct of this study are as follows:

Control Points. Number of control points of the Bézier curve depends on the complexity of the signature being approximated. Sometimes, it is easier to manage the curve with fewer points especially when the curve is not that intricate.

Partition. According to Choi (2010), Bézier curves consisting of large number of control points are numerically unstable. With this remark, partitioning of signatures would be necessary.

Step size for t . The necessity of the step size depends on the curves to be approximated. It is best, most of the time, to use smaller step size for the accuracy of every curve.

Degree. The degree of parametric equation of each low-degree Bézier curves depends on the number of control points that defines it. Customarily, the highest degree of Bézier curve being used is not greater than three (Chen, 2007). Computation-wise, it is easy to set-up equations, substitute and compute if the degree of the equation is not very large.

Interval. Points can be chosen in any interval. However, working on very small interval would be disadvantageous when adjusting or smoothening the Bézier curve.

Bézier curve always passes through points P_0 and P_n and the points made are always tangent to the lines connecting P_0 to P_1 , P_n to P_{n-1} at P_0 and P_n . The curves always recline within the convex hull that consists the control points (Choi, 2010).

CONCLUDING REMARKS

Bézier Curves are commonly applied in computer graphics to generate sensibly smooth curves. The smoothness of the curves is managed by selecting appropriate step size and increasing the number of control points to be used. Moreover, partitions in every graph, which in this case is the signature, lessen the labor of formulating lengthy and multipart equations. The degree of every equation depends on the complexity of the signature.

The authors enjoyed the conduct of this activity while appreciating technical mathematics. Although, without statistical experimentation, this activity can also be used as a fun classroom activity in teaching mathematical concepts such as polynomials, Pascal's triangle and combinations, as well as the Cartesian coordinate system.

LITERATURE CITED

- Casselmann B. American Mathematical Society: monthly essays on Mathematical topics. From Bezier to Bernstein [Internet]. [cited 2010 August 23]. Available from: <http://www.ams.org/samplings/feature-column/fcarc-bezier>
- Chabert J et al. A history of algorithms: from the pebble to the microchip [Internet]. Italy: Springer-Verlag Berlin Heidelberg; 1999 [cited 2010 August 23]. Available from: http://books.google.com/books?id=B1c0s3ffN_0C&pg=PA418&dq=Bernstein+polynomial%2Bspecial+type%2Bweierstrass+theorem%2BSergei+Bernstein&hl=en&ei=juG2TJO2CoHvcOfUxPMJ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCgQ6AEwAA#v=onepage&q&f=false
- Chen S. 2007. Quick sampling method for cubic Bezier curves by chordal error. International Journal of Mathematics and Computers in Simulation [Internet]. [cited 2010 August 23];1:279-282. Available from: <http://www.naun.org/journals/mcs/mcs-43.pdf>
- Choi J, Curry R, Elkaim G. 2010. Continuous Curvature Path Generation Based on Bezier Curves for Autonomous Vehicles. IAENG International Journal of Applied Mathematics [Internet]. [cited 2010 August 23];40(2):4. Available from: http://www.iaeng.org/IJAM/issues_v40/issue_2/IJAM_40_2_07.pdf