IJABER, Vol. 14, No. 2 (2016): 1291-1302

ON CRYPTOGRAM: BUILDING APPRECIATION OF THE UTILITY OF MATRIX CONCEPTS

Renan P. Limjuco[1]

Abstract: *The lack of interest of students in mathematics is caused by the absence of its concrete applications for everyday life. This issue is common especially in matrix concepts. Thus, this study aimed to showcase a fascinating application of matrices called cryptogram. A cryptogram is a message written so that no one other than the intended recipient can understand it. To encode a message, one assigns a number to each letter in the alphabet: A = 1, B = 2, C = 3, …, Z = 26, and a space = 0. The numerical equivalent of the message is then converted into a matrix. An invertible matrix can be used to convert the message into code. The multiplicative inverse of this matrix can be used to decode the message. This investigation dealt with the concepts of cryptogram encoding and decoding. Twenty-five students were given some messages to convert and encode and also twenty-five acted as recipients of the coded messages, who were tasked to decode them. After the exercise, the McNemar's Change Test was employed to assess the degree of appreciation for the utility of the matrix concepts. Findings of the study revealed a significant change in the evaluation of the students in favor of their appreciation of application.*

Keywords: *Mathematics, cryptogram, encode, decode, matrix concepts, focus group discussion, McNemar's change*

INTRODUCTION

Background of the Study

Creative learning suggests that one never stops learning and that one never stops learning how to learn. In other words, learning at its best is a creative, playful adventure, in which the individual is constantly exploring new ways of doing things and pushing back the boundaries of what is possible. This is far removed from the dull practices of rote-learning and slavish adoption of approved 'study technique'. We are creative when we take particular thoughts and ideas and connect them together in a novel way so as to produce something which is fresh, interesting and possibly valuable (Creativity, 2011).

1. University of the Immaculate Conception, Davao City, Philippines *Email: ren02lim@gmail.com*

According to Felder and Silverman (1988), students preferentially take in and process information in different ways, such as by seeing and hearing, reflecting and acting, reasoning logically and intuitively, or by analyzing and visualizing. Thus, teaching methods must also be varied to cater different learners. Some instructors lecture, others demonstrate or lead students to self-discovery; some focus on principles and others on applications. When mismatches exists between learning styles of most students in a class and the teaching style of the professor, the students may become bored and inattentive in class, do poorly on tests, get discouraged about the courses, the curriculum, and themselves, and in some cases change to other curricula or drop out of school. To overcome these problems, professors should strive for a balance of instructional methods. If the balance is achieved, all students will be taught partly in a manner they prefer, which leads to an increased comfort level and willingness to learn, and partly in a less preferred manner, which provides practice and feedback in ways of thinking and solving problems which they may not initially be comfortable with but which they will have to use to be fully effective professional (Learning Styles, 2011).

Moreover, there have been considerable interests to understand the appreciation behavior among mathematics learners to look for possible ways to improve performance. Math appreciation (learning maturation), a construct approximated by math maturity as defined by Moursund (2004), is brought about by a lot of things. It could be influenced by understanding, problem solving, theorem proving, precise mathematical communication, mathematical logic and reasoning, knowing how to learn math, problem posing, transfer of learning (being able to use one's mathematical knowledge over a wide range of disciplines and in novel settings) and interest (including intrinsic motivation) in math (Moursund, 2004). However, there are students who love mathematics because they have learned its structure immediately like a language. Thus, these students usually are recognized as the mathematically gifted ones. To them, mathematics is everything defined by its nature--- sequential, developmental, intuitive, and difficult. Therefore, to the mathematically gifted ones, mathematics is just what really it is. Learners either love it or hate it.

Appreciating mathematical structure, and making use of it, is not a technique or a procedure to be taught alongside addition and subtraction. Rather, mathematical structure is an awareness which, if developed in and for students, will transform their mathematical thinking and their disposition to engage in it. This can only happen if teachers themselves become not only aware of structural relationships, but also have at hand strategies and tactics such as those described in this paper for bringing structural relationships to the fore. It is maintained that this belief applies at every age.

In consideration of the above, one possible strategy to increase learners' appreciation of math concept is the use of matrix concepts in cryptogram. A cryptogram is a message written so that no one other than the intended recipient can understand it; though it can be encoded to bring back the original message (Blitzer, 2010). In particular it is a type of puzzle that consists of a short piece of encrypted text. Generally the cipher used to encrypt the text is simple enough that cryptogram can be solved by hand. Frequently used are substitution ciphers where each letter is replaced by a different letter or number. To solve the puzzle, one must recover the original lettering. Though once used in more serious applications, they are now mainly printed for entertainment in newspapers and magazines.

One of the fascinating applications of matrix concepts is seen in cryptography, specifically in cryptograms. The following passage illustrates the most common utility of such math concepts in reality.

A cryptogram is a massage written so that no one other than the intended recipient can understand it. To encode a message requires assigning a number to each letter in the alphabet: $A = 1$, $B = 2$, $C = 3,\ldots, Z = 26$, and a space = 0. For example, the numerical equivalent of the word MATH is 13, 1, 20, and 8. The numerical equivalent of the message is then converted into a matrix. Finally, an invertible matrix can be used to convert the message into code. The multiplicative inverse of this matrix can be used to decode message (Blitzer, 2004). Mathematically, the process is understood as follows:

The matrix equation $AX = B$ can be solved using A-1 if it exists.

$AX = B$	This is the matrix equation
$A^{-1} AX = A^{-1} B$	Multiply both sides by A^{-1}. Because matrix multiplication is not commutative, put A^{-1} in the same left position on both sides.
$In\ X = A^{-1} B$	The multiplicative inverse property tells us that $A^{-1} A = In$
$X = A^{-1} B$	Because In is the multiplicative identity, $I_n X = X$.

Thus, it can be seen that if $AX = B$, then $X = A$-$1\ B$.

In particular, the following sets of instructions outline the infused cryptogram-related exercises used in this investigation.

Figure 1: Basic steps of encoding and decoding a message

Encoding a Word or Message

1. Express the word or message numerically.
2. List the numbers in step 1 by columns and form a square matrix. Put zeros in any remaining spaces in the last column.
3. Select any square invertible matrix, called the coding matrix, the same size as the matrix in step 2. Multiply the coding matrix by the square matrix that expresses the message numerically. The resulting matrix is the coded matrix.
4. Use the numbers, by columns, from the coding matrix in step 3 to write the encoded matrix.

Decoding a Word or Message that was Encoded

1. Find the multiplicative inverse of the coding matrix.
2. Multiply the multiplicative inverse of the coding matrix and the coded matrix.
3. Express the numbers, by columns, from the matrix in step 2 as letters.

Objectives of the Study

The primary aim of this investigation was to describe the mathematical nature and structure of cryptogram to promote creative and experiential mathematics instruction. Specifically, the researcher attempted to showcase a fascinating application of matrices called cryptogram, measure the degree of appreciation of matrix concepts by math students through the infusion of cryptogram as a classroom activity, and explore the possibility of enriching the learning of matrix concepts through a concrete classroom activity through cryptogram coding and encoding.

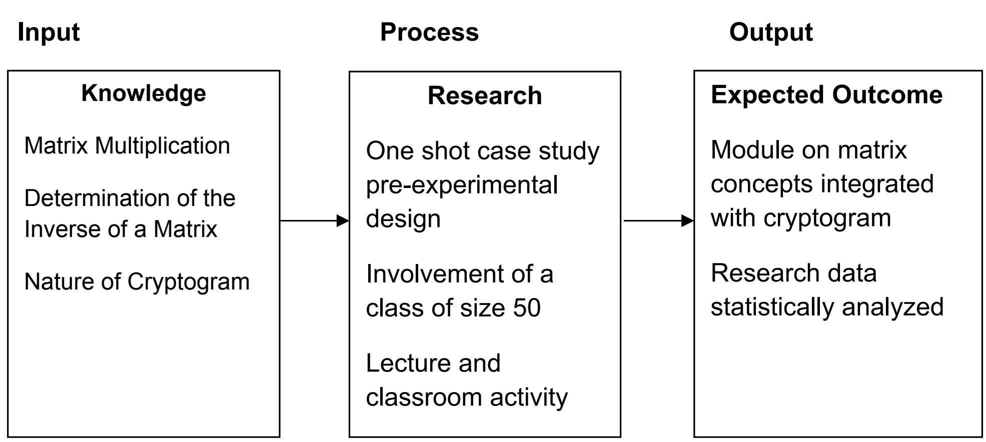
Theoretical Framework

This study is anchored on the concept of constructivism, which points out the need to increase the level of self-motivation and personal involvement among learners. In mathematics, a constructivist always seeks to impact deeper comprehension of the subject matter (Vygotsky, 1978; Vygotsky, 1986; Crawford & Deer, 1993). This job is often channeled to math teachers to realize through the infusion of enriched learning activities in their usual curriculum inside the classroom (Confrey, 1990). These student-centered curricular trends uphold the idea that effective instruction is not achieved by explaining how students take in and process information transmitted by the teacher. Instead, it is to explain how students actively construct knowledge in ways that satisfy constraints inherent in instruction (Cobb 1988). To support this premise, Hodges and Conner (2011) have also advocated the idea that students' identification with mathematics is heightened by focusing on the role of a mathematics teacher in a technology-rich classroom. They believe that an important consideration in understanding students' identification with mathematics is the extent to which activities are designed to be learner-centered using available technologies in the classroom and how the teachers use them to craft learning opportunities for students (Hodges and Conners, 2011).

Also, the Social Learning Theory explains that human development is best described as a continuous reciprocal interaction between children and their environments: the environment clearly affects the child, but the child's behavior is thought to affect the environment as well (Gines: Developmental Psychology 1998). Lastly, the Discovery learning is an inquiry-based learning theory that takes place in problem solving situations where the learner draws on his or her own past experience and existing knowledge to discover facts and relationship and new truths to be learned. Students interact with the world by exploring and manipulating objects, wrestling with questions and controversies, or performing experiments. As a result, students may be more likely to remember concepts and knowledge discovered on their own (in contrast to a transmissionist model). Models that are based upon discovery learning model include: guided discovery, problem-based learning, simulation-based learning, case-based learning, incidental learning, among others (Bruner, 2012).

Conceptual Framework

Figure 2: Conceptual framework of the study



As shown by Figure 2, the input-process-output model was implemented to describe the utility of matrix concepts in cryptogram. In assessing the appreciation of the connectivity among the various matrix operations and the cryptogram and the learning value, basic knowledge on matrix multiplication, determination of the inverse of a matrix, and understanding of the nature of cryptogram are the essential elements to make up the requisite knowledge the participants have to possess to realize this model's input. The process involves a one-shot case study involving a pre-experimental design to involve a relatively medium-sized class to undergo the prescribed activity. This intervention is necessary to generate quantitative data to establish appreciation and validate class activity feasibility. Based on the results of the research are the practical modules or some set of statistically analyzed data to support claims of performance effectiveness or to discuss implications for pedagogy.

METHOD

Research Design

The researcher used a pre-experimental design, specifically the one shot case study. This approach is implemented if the attempt of the study is to explain a consequence by an antecedent. In this investigation, a straightforward lecture on cryptogram involving encoding and decoding messages followed by a clearly designed classroom activity was conducted and the feedback from the participants by way of the counts of successful cases as described in the procedure was taken as the outcome to assess appreciation.

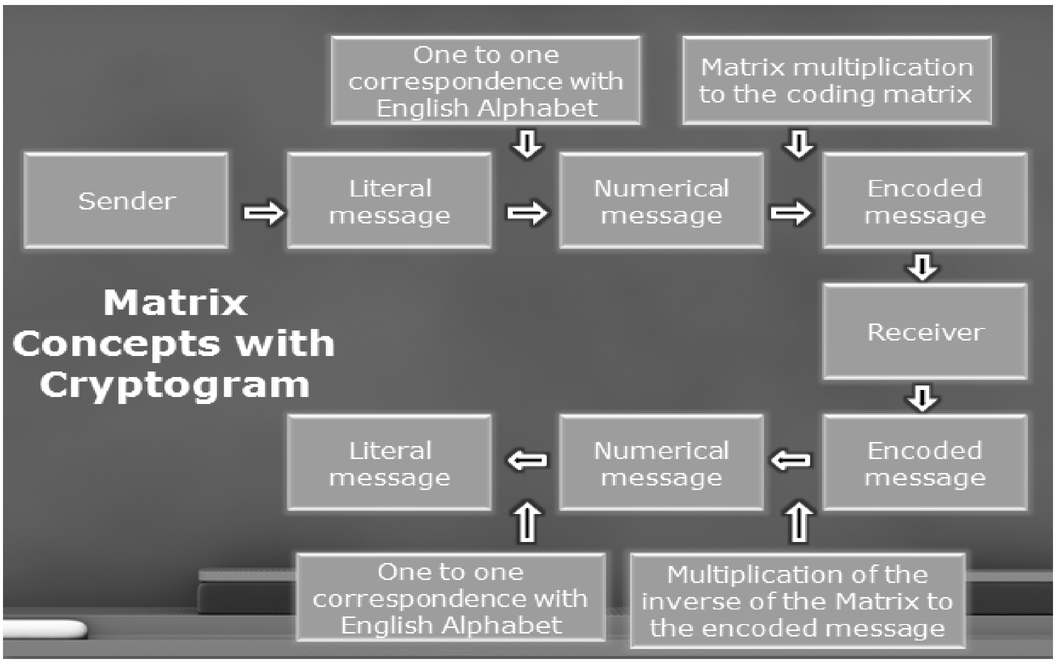
Research Locale, Participants, and Sampling

One Advanced Algebra class of 50 students from the Engineering program of the University of the Immaculate Conception was purposively chosen. The researcher considered the following criteria: being BS Electronics Engineering students, having finished and mastered the topics on matrices, especially matrix multiplication and inverse of matrix determination, and having been oriented on the nature of cryptogram and how the matrix concepts are embedded into it.

Research Procedure

Twenty-five students were given some messages to convert and encode and also correspondingly 25 acted as recipients of the coded messages, who were then tasked to decode them. In other words, 25 pairs were under observation as they implement the following procedure:

Figure 3: Procedure for class activity on cryptogram utilization of matrix concepts



Each of the 25 students identified as senders was given a unique message to be converted from literal to numerical symbols using the 1-1 correspondence involving the English alphabet, that is, A = 1, B = 2, … Z = 26, fitting them into a square matrix. Then, they were instructed to produce their own encoded message (B) by multiplying it (X = the numerical message) to a pre-determined invertible coding matrix (A). Mathematically, it must be made sure that $AX = B$. The designated receiver, then, would multiply the inverse of the coding matrix (A-1) and the encoded message (B) to get back X. Finally, using the 1-1 correspondence, the original message was revealed.

The researcher employed the McNemar Change Test to assess the extent of appreciation of the students of the utility of matrix concepts in cryptogram. McNemar change Test assesses the significance of the difference between two correlated proportions, such as might be found in the case where the two proportions are based on the same sample of subjects or on matched-pair samples. In this study, the proportions of students who appreciated the matrix operations, specifically the inverse of matrix determination, before and after the cryptogram-infused classroom activity, were compared to determine the significance of the change in proportions.

RESULTS AND DISCUSSION

The following subsections elucidate the learning activities that were implemented in the intervention done for this study. Applications of matrix concepts involving multiplication of square matrices and the determination of the inverses of given invertible matrices are highlighted. Eventually, some data to establish performance of students in matrix operations as well as the change in the proportions of the students who appreciate the utilization of matrix operations in cryptogram before and after the classroom activity are explained.

Infused Cryptogram-Related Activities in Initial Phase: Encoded and Decoded Messages

Table 1 reveals three of the specimens of messages which were used by the students in the preliminary activities. The specimen messages HOW ARE YOU and SEND CASH were processed using a 3 x 3 coding matrix A whose elements R_1 = 1, 0, 3; R_2 = 2, 2, 2; R_3 = 1, 2, 1 with its corresponding inverse A^{-1} whose elements R_1 = - 0.5, 1.5, - 1.5; R_2 = 0, - 0.5, 1; R_3 = 0.5, -0.5, 0.5. On the other hand, the specimen message ARRIVED SAFELY was encoded and decoded with the use of a 4 x 4 coding matrix A whose elements R_1 = 2, 0, 1, 1; R_2 = 3, 0, 0, 1; R_3 = -1, 1, -2, 1; R_4 = 4, -1, 1, 0 with its corresponding inverse A^{-1} whose elements R_1 = -1, 2, -1, -1; R_2 = -4, 9, -5, -6; R_3 = 0, 1, -1, -1 and R_4 = 3, -5, 3, 3. Basically, the activity involved multiplication of matrices and converting literal messages into numerical messages through a 1 to 1 correspondence from English alphabet and natural numbers, that is, A = 1, B = 2, C = 3,… Z = 26. A space used 0 to complete the square matrix required.

Going consistently row-wise in placing the letters in the matrices, the message HOW ARE YOU was encoded as 83, 60, 86, 68, 96, 98, 35, 66, 54 and was successfully decoded as 8, 15, 23, 1, 18, 5, 25, 21 by 20 out of 25 pairs of students. Similarly the message SEND CASH was encoded as 22, 62, 38, 48, 48, 50, 28, 24, 28 which was decoded successfully by the 25 pairs.

As shown by Table 1, the message ARRIVED SAFELY, encoded as 33, 62, 42, 23, 15, 79, 54, 27, -5, 10, 26, -19, 1, 68, 74, 41 and decoded as 1, 18, 18, 9, 22, 5, 4, 0, 19, 1, 6, 5 was successfully processed at 21 out of 25.

Table 1
Encoded and Decoded Messages Using Coding and Inverse of Coding Matrices in Initial Phase

Message Specimen	*Numerical Message, X*	*Coding Matrix, A*	*Encoded Message, B=AX*	*Inverse of Coding Matrix, A^{-1}*	*Decoded Message, $X=A^{-1}B$*	*Success Rate*
HOW ARE YOU	$\begin{bmatrix} 8 & 15 & 23 \\ 1 & 18 & 5 \\ 25 & 15 & 21 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 83 & 60 & 86 \\ 68 & 96 & 98 \\ 35 & 66 & 54 \end{bmatrix}$ 83, 60, 86, 68, 96, 98, 35, 66, 54	$\begin{bmatrix} -0.5 & 1.5 & -1.5 \\ 0 & -0.5 & 1 \\ 0.5 & -0.5 & 0.5 \end{bmatrix}$	$\begin{bmatrix} 8 & 15 & 23 \\ 1 & 18 & 5 \\ 25 & 15 & 21 \end{bmatrix}$ 8, 15, 23, 1, 18, 5, 25, 15, 21	$\frac{20}{25}$
SEND CASH	$\begin{bmatrix} 9 & 5 & 14 \\ 4 & 0 & 3 \\ 1 & 19 & 8 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 2 & 2 & 2 \\ 1 & 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 22 & 62 & 38 \\ 48 & 48 & 50 \\ 28 & 24 & 28 \end{bmatrix}$ 22, 62, 38, 48, 48, 50, 28, 24, 28	$\begin{bmatrix} -0.5 & 1.5 & -1.5 \\ 0 & -0.5 & 1 \\ 0.5 & -0.5 & 0.5 \end{bmatrix}$	$\begin{bmatrix} 9 & 5 & 14 \\ 4 & 0 & 3 \\ 1 & 19 & 8 \end{bmatrix}$ 19, 5, 14, 4, 0, 3, 1, 19, 8	$\frac{25}{25}$
ARRIVED SAFELY	$\begin{bmatrix} 1 & 18 & 18 & 9 \\ 22 & 5 & 4 & 0 \\ 19 & 1 & 6 & 5 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 & 1 & 1 \\ 3 & 0 & 0 & 1 \\ -2 & 1 & -2 & 1 \\ 4 & -1 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 33 & 62 & 42 & 23 \\ 15 & 79 & 54 & 27 \\ -5 & 10 & 26 & -19 \\ 1 & 68 & 74 & 41 \end{bmatrix}$ 33, 2, 42, 23, 15, 79, 54, 27, -5, 10, 26, -19, 1, 68, 74, 41	$\begin{bmatrix} -1 & 2 & -1 & -1 \\ -4 & 9 & -5 & -6 \\ 0 & 1 & -1 & -1 \\ 3 & -5 & 3 & 3 \end{bmatrix}$	$\begin{bmatrix} 18 & 18 & 9 \\ 5 & 4 & 0 \\ 1 & 6 & 0 \\ 68 & 74 & 41 \end{bmatrix}$ 1, 18, 18, 9, 22, 5, 4, 0, 19, 1, 6, 5	$\frac{21}{25}$

Table 2
Performance of Students in Matrix Concepts with Cryptogram in Final Phase

Pairs of Learners	*Percentage of Good Performance*	*Senders*		*Receivers*	
		Succeeded	*Failed*	*Succeeded*	*Failed*
23 (46 students)	92	23	0	23	0
2 (4 students)	8	2	0	0	2

Measure of Students' Skills in Encoding and Decoding a Cryptogram in Final Phase

Table 2 reveals the level of skills of student participants in encoding-decoding activities for the final phase. Out of 25 pairs, only 2 pairs failed to process their own secret messages. This one shot data set implies a performance of 92%. It can be inferred that the students have already attained a stable knowledge and skills in matrix operations specifically, on matrix multiplication and inverse of the matrix determination. During the post discussion, the two students, assigned as receivers, who failed to decode the message realized that the mistakes were due to carelessness only.

Table 3
Testing the Significance of Appreciation through McNemar Change Test

		After the class exercise		*Chi-Square Tabular @ $df = 1$; $\alpha = 0.01$*	*Chi-Square Calculated*	*p-value (2-tailed)*	*Decision*
		Not Appreciative	*Appreciative*				
Before the class exercise	Appreciative	1	15	6.64	11.53	0.00069	significant
	Not Appreciative	18	16				

In testing whether the exposure of student participants to classroom activities infused with cryptogram-related exercises can increase the proportion of the appreciative learners with respect to the nature and mathematical structure of cryptogram, McNemar Change Test was implemented by the researcher. As Table 3 reveals, the number of appreciative students has increased from 16 before the class activities to 31 after the intervention. In the analysis, out of 34 students who initially were not appreciative of the matrix concepts, only 18 remained firm in their judgment. Thus, the matrix concepts and the relevant matrix operations infused with cryptogram-related exercises have built an increased level of appreciation among math students (p-value < 0.01).

This encouraging result is supported by the beliefs of Hodges and Conner (2011) who advocated the idea that students' identification with mathematics is heightened by focusing on the role of a mathematics teacher in a technology-rich classroom. They believe that an important consideration in understanding students' identification with mathematics is the extent to which activities are designed to be learner-centered using available technologies in the classroom and how the teachers use them to craft learning opportunities for students (Hodges and Conners, 2011).

CONCLUSION

The mathematics students have improved their skills in matrix multiplication and matrix inverse determination due to the more enriched learning activity that concretizes the matrix concepts through an application in cryptogram. After the learning activities, a significant increase in the proportion of appreciative students on matrix concepts due to the inclusion of cryptogram in the technicalities of matrix multiplication and matrix inverse determination was manifested. This scenario proves once more that the constructivists' perspectives are true and highly manifested in learner-centered classroom environment. Thus, the teaching of matrix multiplication and matrix inverse determination needs concretization through the introduction of some useful applications like cryptogram encoding and decoding making use of the said concepts. As implications for educational practice, math teachers infuse the topics on matrix multiplication and matrix inverse determinations with encryption and decryption techniques to increase the appreciation of math students to abstract techniques of mathematics.

References

Blitzer, R (2010). *Algebra and Trigonometry*. Addison Wesly Publishing Company Incorporated

Bruner, J. (2014). Learning Theories. http://www.learning-theories.com/discovery-learning-bruner.html

Cobb, P. (1988). *The tension between theories of learning and instructions in Mathematics education.* Educational Psychologist. 23 (2); 87-103.

Confrey, J. (1990). *What constructivism implies for teaching*. Journal for Research in Mathematics Education Mono graph 4, 1990.

Crawford, K. and C.E. Deer. (1993). *Do we practice what we preach?* Putting policy into practice in teacher education. South Pacific Journal of Teacher Education, 21 February 1993, 111-121.

Creativity (2011). *Creative learning,* 19 December 2011. http://www.jwelford. demon.co.uk/brainwaremap.html

Felder, R.M. and Silverman, L.K. (1988). *"Learning and Teaching Styles in Engineering Education,"* Engr. Education 78(7), 674-681.

Gines, A. (1998). *Developmental Psychology.* Rex Printing Company, Inc.

Hodges T.E. and E. Conner. (2011). *Reflection on a technology-rich mathematics classroom.* The Mathematics Teacher. February 2011, 432.

Learning Styles (2011). *Learning styles,* 19 December 2011. http://www4.ncsu. edu/unity/lockers/users/f/felder/public/Learning_Styles.html

Moursund, Dave (2004). Increasing the Math Maturity of Elementary School Students and Their Teachers 24 December 2011 http://darkwing. uoregon.edu/-moursund/Math/.

Vygotsky, L.S. (1978). *Mind and Society: The Development of Higher Mental Process*. Cambridge, MA: Harvard University Press.

Vygotsky, L.S. (1986). *Thought and Language*. Cambridge (Mass): MIT Press.