Exact Distribution of the Max/Min of Two Gaussian Random Variables

Saralees Nadarajah and Samuel Kotz

***Abstract*—Maximum and minimum of correlated Gaussian random variables arise naturally with respect to statistical static time analysis. It appears, however, that only approximations have been used in the recent literature to study the distribution of the max/min of correlated Gaussian random variables. In this paper, we would like to point out that the statistics literature has long established simple expressions for the exact distribution of the max/min. We provide some of the known expressions for the following: the probability density function, moment generating function, and the moments. We also provide two simple programs for computing the probability density functions of the max/min and an illustration of the results to statistical static time analysis.**

***Index Terms*—Maximum, minimum, moment generating function (MGF), moments, probability density function (pdf), statistical static time analysis (SSTA).**

I. Introduction

Let (X_1, X_2) denote a bivariate Gaussian random vector with means (μ_1, μ_2), variances (σ_1^2, σ_2^2), and correlation coefficient ρ. The distributions of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$ have a prominent role with respect to statistical static time analysis (SSTA). It appears, however, that most SSTA researchers use certain approximations to study the distributions of X and Y (see [1]–[7]).

We would like to point out that simple expressions for the exact distributions of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$ have long been known in the statistics literature, see Basu and Ghosh [8], Nagaraja and Mohan [9], David [10], and Tong [11]. In this paper, we provide some of the known properties of X and Y for the use of SSTA researchers. Section II provides the probability density functions (pdf), Section III provides the moment generating functions (MGFs), Section IV provides some of the moments, and Section V provides two simple programs for computing the pdfs of X and Y. Finally, an illustration of these results to SSTA is given in Section VI. It is expected that the results of this paper could be useful with respect to modeling problems involving maximum and minimum of correlated Gaussian random variables.

II. PDFs of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$

It is known that the pdf of $X = \max(X_1, X_2)$ is $f(x) = f_1(-x) + f_2(-x)$, where

$$f_1(x) = \frac{1}{\sigma_1}\phi\left(\frac{x+\mu_1}{\sigma_1}\right) \times \Phi\left(\frac{\rho(x+\mu_1)}{\sigma_1\sqrt{1-\rho^2}} - \frac{x+\mu_2}{\sigma_2\sqrt{1-\rho^2}}\right) \quad (1)$$

$$f_2(x) = \frac{1}{\sigma_2}\phi\left(\frac{x+\mu_2}{\sigma_2}\right) \times \Phi\left(\frac{\rho(x+\mu_2)}{\sigma_2\sqrt{1-\rho^2}} - \frac{x+\mu_1}{\sigma_1\sqrt{1-\rho^2}}\right) \quad (2)$$

Manuscript received March 12, 2007; revised March 19, 2007.

S. Nadarajah is with the University of Manchester, Manchester M60 1QD, U.K (e-mail: saralees.nadarajah@manchester.ac.uk).

S. Kotz is with the George Washington University, Washington, D.C. 20052 USA.

Digital Object Identifier 10.1109/TVLSI.2007.912191

where $\phi(\cdot)$ and $\Phi(\cdot)$ are, respectively, the pdf and the cumulative distribution function (cdf) of the standard normal distribution. It is known that the pdf of $Y = \min(X_1, X_2)$ is $f(y) = f_1(y) + f_2(y)$, where

$$f_1(y) = \frac{1}{\sigma_1}\phi\left(\frac{y-\mu_1}{\sigma_1}\right) \times \Phi\left(\frac{\rho(y-\mu_1)}{\sigma_1\sqrt{1-\rho^2}} - \frac{y-\mu_2}{\sigma_2\sqrt{1-\rho^2}}\right) \quad (3)$$

$$f_2(y) = \frac{1}{\sigma_2}\phi\left(\frac{y-\mu_2}{\sigma_2}\right) \times \Phi\left(\frac{\rho(y-\mu_2)}{\sigma_2\sqrt{1-\rho^2}} - \frac{y-\mu_1}{\sigma_1\sqrt{1-\rho^2}}\right). \quad (4)$$

III. MGFs of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$

It is known that the mgf of $X = \max(X_1, X_2)$ is $m(t) = m_1(-t) + m_2(-t)$, where

$$m_1(t) = \exp\left(-t\mu_1 + \frac{t^2\sigma_1^2}{2}\right) \times \Phi\left(\frac{\mu_1 - \mu_2 - t\left(\sigma_1^2 - \rho\sigma_1\sigma_2\right)}{\theta}\right) \quad (5)$$

$$m_2(t) = \exp\left(-t\mu_2 + \frac{t^2\sigma_2^2}{2}\right)! \times \Phi\left(\frac{\mu_2 - \mu_1 - t\left(\sigma_2^2 - \rho\sigma_1\sigma_2\right)}{\theta}\right) \quad (6)$$

where $\theta = \sqrt{\sigma_1^2 + \sigma_2^2 - 2\rho\sigma_1\sigma_2}$. It is known that the mgf of $Y = \min(X_1, X_2)$ is $m(t) = m_1(t) + m_2(t)$, where

$$m_1(t) = \exp\left(t\mu_1 + \frac{t^2\sigma_1^2}{2}\right) \times \Phi\left(\frac{\mu_2 - \mu_1 - t\left(\sigma_1^2 - \rho\sigma_1\sigma_2\right)}{\theta}\right) \quad (7)$$

$$m_2(t) = \exp\left(t\mu_2 + \frac{t^2\sigma_2^2}{2}\right) \times \Phi\left(\frac{\mu_1 - \mu_2 - t\left(\sigma_2^2 - \rho\sigma_1\sigma_2\right)}{\theta}\right) \quad (8)$$

where $\theta = \sqrt{\sigma_1^2 + \sigma_2^2 - 2\rho\sigma_1\sigma_2}$.

IV. Moments of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$

The moments of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$ of any order can be obtained by differentiating (5)–(8). For instance, it is known that the first two moments of $X = \max(X_1, X_2)$ are

$$E(X) = \mu_1\Phi\left(\frac{\mu_1-\mu_2}{\theta}\right) + \mu_2\Phi\left(\frac{\mu_2-\mu_1}{\theta}\right) + \theta\phi\left(\frac{\mu_1-\mu_2}{\theta}\right) \quad (9)$$

$$E(X^2) = \left(\sigma_1^2 + \mu_1^2\right)\Phi\left(\frac{\mu_1-\mu_2}{\theta}\right) + \left(\sigma_2^2 + \mu_2^2\right)\Phi\left(\frac{\mu_2-\mu_1}{\theta}\right) + (\mu_1+\mu_2)\,\theta\phi\left(\frac{\mu_1-\mu_2}{\theta}\right) \quad (10)$$

where $\theta = \sqrt{\sigma_1^2 + \sigma_2^2 - 2\rho\sigma_1\sigma_2}$. The first two moments of $Y = \min(X_1, X_2)$ are

$$E(Y) = \mu_1\Phi\left(\frac{\mu_2-\mu_1}{\theta}\right) + \mu_2\Phi\left(\frac{\mu_1-\mu_2}{\theta}\right) - \theta\phi\left(\frac{\mu_2-\mu_1}{\theta}\right) \quad (11)$$

$$E(Y^2) = \left(\sigma_1^2 + \mu_1^2\right)\Phi\left(\frac{\mu_2-\mu_1}{\theta}\right) + \left(\sigma_2^2 + \mu_2^2\right)\Phi\left(\frac{\mu_1-\mu_2}{\theta}\right) - (\mu_1+\mu_2)\,\theta\phi\left(\frac{\mu_2-\mu_1}{\theta}\right) \quad (12)$$

where $\theta = \sqrt{\sigma_1^2 + \sigma_2^2 - 2\rho\sigma_1\sigma_2}$.

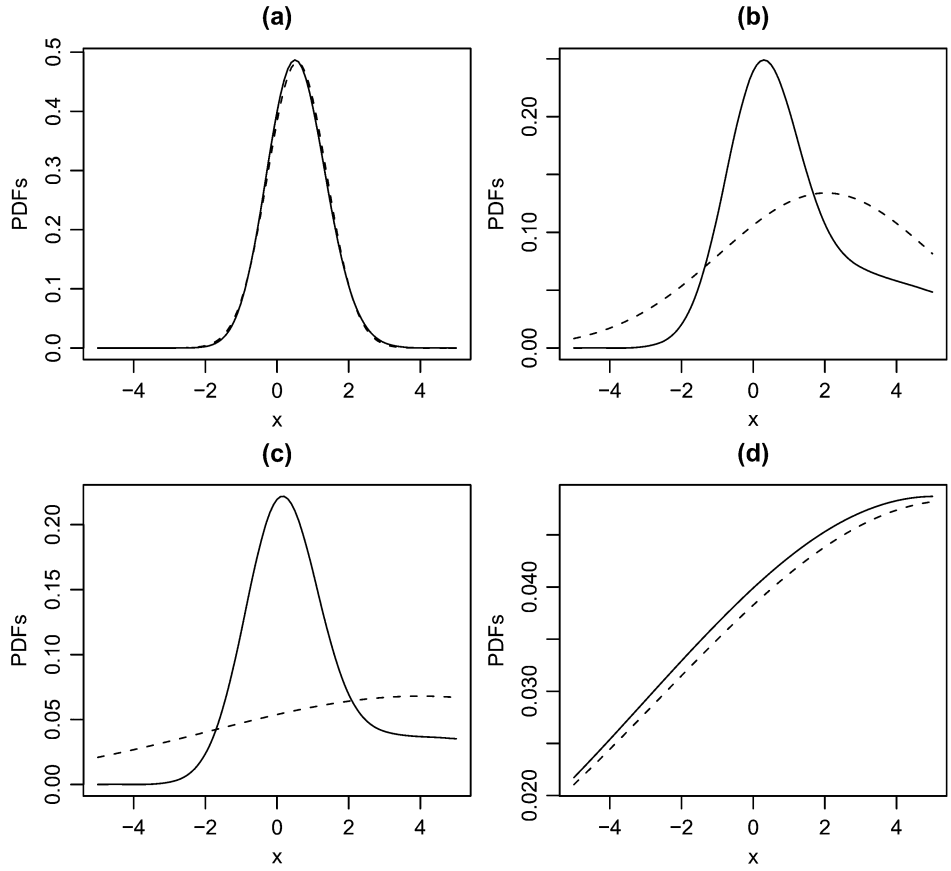

Fig. 1. Comparison of the pdf of $X = \max(X_1, X_2)$ with its Gaussian approximation for: (a) $\mu_1 = \mu_2 = 0, \sigma_1 = 1$, and $\sigma_2 = 1$; (b) $\mu_1 = \mu_2 = 0, \sigma_1 = 1$, and $\sigma_2 = 5$; (c) $\mu_1 = \mu_2 = 0, \sigma_1 = 1$, and $\sigma_2 = 10$; and (d) $\mu_1 = \mu_2 = 0, \sigma_1 = 10$, and $\sigma_2 = 10$. The solid and the broken curves correspond to the pdfs of $X = \max(X_1, X_2)$ and its Gaussian approximation, respectively.

V. Programs for Computing the PDFs of X and Y

Here, two simple functions are given for computing the pdfs, $f(x)$ and $f(y)$, of $X = \max(X_1, X_2)$ and $Y = \min(X_1, X_2)$, respectively. The call to the function fmax (x, mu1, mu2, sigma1, sigma2, rho) will return the value of $f(x)$ for given $x, \mu_1, \mu_2, \sigma_1, \sigma_2$ and ρ. The call to the function fmin (y, mu1, mu2, sigma1, sigma2, rho) will return the value of $f(y)$ for given $y, \mu_1, \mu_2, \sigma_1, \sigma_2$, and ρ.

```
fmax<-function (x,mu1,mu2,sigma1,sigma2,rho)
{t1<-dnorm(-x,mean= -mu1,sd=sigma1)
tt<-rho*(mu1-x)/(sigma1*sqrt(1-rho*rho))
tt<-tt-(mu2-x)/(sigma2*sqrt(1-rho*rho))
t1<-t1*pnrom(tt)
t2<-dnorm(-x,mean= -mu2,sd=sigma2)
tt<-rho*(mu2-x)/(sigma2*sqrt(1-rho*rho))
tt<-tt-(mu1-x)/(sigma1*sqrt(1-rho*rho))
t2<-t2*pnrom(tt)
return(t1+t2)}

fmin<-function (y,mu1,mu2,sigma1,sigma2,rho)
{t1<-dnorm(y,mean=mu1,sd=sigma1)
tt<-rho*(y-mu1)/(sigma1*sqrt(1-rho*rho))
tt<-tt-(y-mu2)/(sigma2*sqrt(1-rho*rho))
t1<-t1*pnrom(tt)
t2<-dnorm(y,mean=mu2,sd=sigma2)
tt<-rho*(y-mu2)/(sigma2*sqrt(1-rho*rho))
tt<-tt-(y-mu1)/(sigma1*sqrt(1-rho*rho))
t2<-t2*pnrom(tt)
return(t1+t2)}
```

Both functions are written in R (R Development Core Team [12]) because, unlike other statistical software, it is freely downloadable from the Internet (http://www.r-project.org) (see also Ihaka and Gentleman [13]). The electronic version of the functions can be obtained by contacting S. Nadarajah.

VI. Illustration

SSTA is a method of computing the expected timing of a digital circuit without requiring simulation. This requires the distribution of the arrival time in circuits given the distributions of each block delay in the circuit. The overall time delay distribution entails consideration of two operations: 1) if X_1 is the input arrival time and X_2 is the block delay then the output arrival time will be $X_1 + X_2$ and 2) if X_1 and X_2 are two arrival times that merge in a block then the new arrival time will be $\max(X_1, X_2)$. The most common assumption is that X_1 and X_2 are independent Gaussian random variables. In this case, it is well known that $X_1 + X_2$ will also have the Gaussian distribution. The distribution of $\max(X_1, X_2)$, described in Sections II–IV, will not be Gaussian. However, as mentioned in Section I, often an approximation is used to study the distribution of $X = \max(X_1, X_2)$. Most commonly, it is assumed that $X = \max(X_1, X_2)$ is Gaussian distributed with the first two moments given by (9) and (10), respectively. Here, we would like to show how poor this approximation can be.

In Fig. 1, we have plotted the pdfs given by (1) and (2) and that of the Gaussian approximation for a range of values of σ_1 and σ_2. We have used the R programs given in Section V. It is clear that the approximation performs very poorly when the standard deviations are not equal. It appears that the approximation gets poorer as the difference between the two standard deviations gets larger. The approximation appears reasonable only when the standard deviations are equal and small.

In SSTA, one also encounters variables of the form $X = \max(\max(X_1, X_2), X_3), X = \max(\max(\max(X_1, X_2), X_3), X_4)$, and so on. The exact distributions of these variables can also be calculated. For example, if $\max(X_1, X_2)$ and X_3 are assumed independent then the pdf and the cdf of $X = \max(\max(X_1, X_2), X_3)$ will be

$$f_X(x) = F_{\max(X_1,X_2)}(x) f_{X_3}(x) + f_{\max(X_1,X_2)}(x) F_{X_3}(x)$$
$$F_X(x) = F_{\max(X_1,X_2)}(x) F_{X_3}(x)$$

respectively. If $\max(X_1, X_2)$ and X_3 are not independent then expressions similar to those in Sections II–IV could be obtained by assuming that (X_1, X_2, X_3) follows the trivariate normal distribution.

REFERENCES

[1] H. Eriksson, P. Larsson-Edefors, and D. Eckerbert, "Toward architecture-based test-vector generation for timing verification of fast parallel multipliers," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 14, no. 4, pp. 370–379, Apr. 2006.

[2] Y. Abulafia and A. Kornfeld, "Estimation of FMAX and ISB in microprocessors," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1205–1209, Oct. 2005.

[3] Y. Cao, X. D. Yang, and X. J. Huang *et al.*, "Switch-factor based loop RLC modeling for efficient timing analysis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 9, pp. 1072–1078, Sep. 2005.

[4] A. Valentian, O. Thomas, and A. Vladimirescu *et al.*, "Modeling subthreshold SOI logic for static timing analysis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 12, no. 6, pp. 662–668, Jun. 2004.

[5] B. Taskin and I. S. Kourtev, "Linearization of the timing analysis and optimization of level-sensitive digital synchronous circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 12, no. 1, pp. 12–27, Jan. 2004.

[6] Y. Cao, X. J. Huang, and N. H. Chang *et al.*, "Effective on-chip inductance modeling for multiple signal lines and application to repeater insertion," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 10, no. 12, pp. 799–805, Dec. 2002.

[7] C. H. Oh and M. R. Mercer, "Efficient logic-level timing analysis using constraint-guided critical path search," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 4, no. 9, pp. 346–355, Sep. 1996.

[8] A. P. Basu and J. K. Ghosh, "Identifiability of the multinormal and other distributions under competing risks model," *J. Multivariate Anal.*, vol. 8, pp. 413–429, 1978.

[9] H. N. Nagaraja and N. R. Mohan, "On the independence of system life distribution and cause of failure," *Scandinavian Actuarial J.*, pp. 188–198, 1982.

[10] H. A. David, *Order Statistics*, 2nd ed. New York: Wiley, 1981.

[11] Y. L. Tong, *The Multivariate Normal Distribution*. New York: Springer-Verlag, 1990.

[12] R Development Core Team, Vienna, Austria, "R: A language and environment for statistical computing, R foundation for statistical computing," ISBN 3-900051-07-0, 2005 [Online]. Available: http://www.R-project.org

[13] R. Ihaka and R. Gentleman, "R: A language for data analysis and graphics," *J. Computational Graph. Stat.*, vol. 5, pp. 299–314, 1996.

FPGA Implementation(s) of a Scalable Encryption Algorithm

F. Macé, F.-X. Standaert, and J.-J. Quisquater

***Abstract*—SEA is a scalable encryption algorithm targeted for small embedded applications. It was initially designed for software implementations in controllers, smart cards, or processors. In this letter, we investigate its performances in recent field-programmable gate array (FPGA) devices. For this purpose, a loop architecture of the block cipher is presented. Beyond its low cost performances, a significant advantage of the proposed architecture is its full flexibility for any parameter of the scalable encryption algorithm, taking advantage of generic VHDL coding. The letter also carefully describes the implementation details allowing us to keep small area requirements. Finally, a comparative performance discussion of SEA with the Advanced Encryption Standard Rijndael and ICEBERG (a cipher purposed for efficient FPGA implementations) is proposed. It illustrates the interest of platform/context-oriented block cipher design and, as far as SEA is concerned, its low area requirements and reasonable efficiency.**

***Index Terms*—Block ciphers, constrained applications, field-programmable gate array (FPGA) implementations, modular design.**

I. INTRODUCTION

Scalable encryption algorithm (SEA) is a parametric block cipher for resource constrained systems (e.g., sensor networks, RFIDs) that has been introduced in [1]. It was initially designed as a low-cost encryption/authentication routine (i.e., with small code size and memory) targeted for processors with a limited instruction set (i.e., AND, OR, XOR gates, word rotation, and modular addition). Additionally and contrary to most recent block ciphers (e.g., the DES [2] and AES Rijndael [3], [4]), the algorithm takes the plaintext, key, *and* the bus sizes as parameters and, therefore, can be straightforwardly adapted to various implementation contexts and/or security requirements. Compared to older solutions for low-cost encryption like tiny encryption algorithm (TEA) [5] or Yuval's proposal [6], SEA also benefits from a stronger security analysis, derived from recent advances in block cipher design/cryptanalysis.

In practice, SEA has been proven to be an efficient solution for embedded software applications using microcontrollers, but its hardware performances have not yet been investigated. Consequently, and as a first step towards hardware performance analysis, this letter explores the features of a low-cost field-programmable gate array (FPGA) encryption/decryption core for SEA. In addition to the performance evaluation, we show that the algorithm's scalability can be turned into a *fully generic* VHDL design, so that any text, key, *and* bus size can be straightforwardly reimplemented without any modification of the hardware description language, with standard synthesis and implementation tools.

In the rest of this paper, we first provide a brief description of the algorithm specifications. Then, we describe the details of our generic loop architecture and its implementation results. Finally, we discuss some illustrative comparisons of the hardware performances of SEA, the AES Rijndael, and ICEBERG (a cipher purposed for efficient FPGA implementations) with respect to their design approach (e.g., flexible versus platform/context-oriented).

Manuscript received November 21, 2006. The work of F. Macé was supported by the FRIA Grant, Belgium. The work of F.-X. Standaert was supported by the Belgian Fund for Scientific Research.

The authors are with the UCL Crypto Group, Laboratoire de Microélectronique, Université Catholique de Louvain, B-1348 Louvain-La-Neuve, Belgium (e-mail: francois.mace@uclouvain.be; fstandae@uclouvain.be; jean-jacques.quisquater@uclouvain.be).

Digital Object Identifier 10.1109/TVLSI.2007.904139