Perl para Sysadmins e DBA"s

Lindolfo "Lorn" Rodrigues
Department of Mathematics, UMIST, Manchester M60 1QD, UK

May 16, 2000

Abstract

You are unlikely to want your research articles to use coloured text but this illustrates how it can be done

KEYWORDS: DPA, ZERO-KNOWLEDGE, INFORMATION THEORY, DISTRIBUTIONS, METRIC

1 Introduction

Zero-Knowledge proofs allow verification of secret-based actions without revealing the secrets. Goldreich et al. [**?**] discussed the class of promise problems in which interaction may give additional information in the context of Statistical Zero-Knowlege. They invoked two types of difference between distributions: the 'statistical difference' and the 'entropy difference' of two random variables. In this context, typically, one of the distributions is the uniform distribution.

Thus, in the contexts of DPA and SZK tests, it is necessary to compare two nearby distributions on bounded domains. We describe the following result and discuss applications.

Proposition 1.1 *The family of probability density functions for random variable* $N \in [0,1]$ *given by*

$$g(N,\mu,\beta) = \frac{\frac{1}{N}^{1-\frac{\beta}{\mu}} (\frac{\beta}{\mu})^{\beta} (\log \frac{1}{N})^{\beta-1}}{\Gamma(\beta)} \quad \text{for } \mu > 0 \text{ and } \beta \geq 1 \tag{1}$$

determines a metric space of distributions with the following properties

- *it contains the uniform distribution*
- *it contains approximations to truncated Gaussian distributions*
- *the difference structure is given by the information-theoretic metric*
- *as a Riemannian 2-manifold it is an isometric isomorph of the manifold of gamma distributions.*

2 In this example

Examples are provided of

1. Coloured text **??**
2. Graphics **??**
3. Tables **??**

3 Proof of Proposition 1.1

3.1 Log-gamma PDFs

By integration, it is easily checked that the family given by equation (**??**) consists of probability density functions for the random variable $N \in [0,1]$; some with central mean are shown in Figure **??**.

n	$\mathbb{S}^n$	$\mathbb{R}^n$
1	1	1
2	1	1
3	1	1
4	1	∞
5	1	1
6	1	1
7	28	1
8	2	1
9	8	1
10	6	1
11	992	1
12	1	1
13	3	1
14	2	1
15	16256	1

Table 1: Numbers of distinct differentiable structures on real n-space and n-spheres

The limiting densities are given by

$$\lim_{\beta\to 1^+} g(N,\mu,\beta) = g(N,\mu,1) \quad = \quad \frac{1}{\mu}\left(\frac{1}{N}\right)^{1-\frac{1}{\mu}} \tag{2}$$

$$\lim_{\mu\to 1} g(N,\mu,1) = g(N,1,1) \quad = \quad 1\ . \tag{3}$$

3.2 Information metric structure

For the log-gamma densities, the Fisher information matrix determines a Riemannian information metric [**?**] on the parameter space $\mathcal{S} = \{(\mu,\beta) \in (0,\infty)\times[1,\infty)\}$. Its arc length function is given by

$$ds^2_{\mathcal{S}} = \sum_{ij} g_{ij}\, dx^i dx^j = \frac{\beta}{\mu^2}\, d\mu^2 + \left(\psi'(\beta) - \frac{1}{\beta}\right)\, d\beta^2, \tag{4}$$

where $\psi(\beta) = \frac{\Gamma'(\beta)}{\Gamma(\beta)}$ is the logarithmic derivative of the gamma function, evaluated at β.
In fact, (**??**) arises from the gamma family

$$f(x,\mu,\beta) = \frac{x^{\beta-1}\,(\frac{\beta}{\mu})^{\beta}}{\Gamma(\beta)}\, e^{-\frac{V\,\beta}{\mu}} \tag{5}$$

for the non-negative random variable $x = \log\frac{1}{N}$. It is known that the gamma family (**??**) has also the information metric (**??**) (cf [**?**]) so the identity map on the space of coordinates (μ,β) is an isometry of Riemannian manifolds. □

4 Tables

Table **??** lists the number of differentiable structures on spheres.
Here is how to set out a table in LaTeX:

```
\begin{table}
\begin{center}
\framebox[1.5in]{\begin{tabular}{c | c | c }
$n$ & $\S^n$ & $\R^n$ \\ \hline
1 & 1 & 1 \\
```

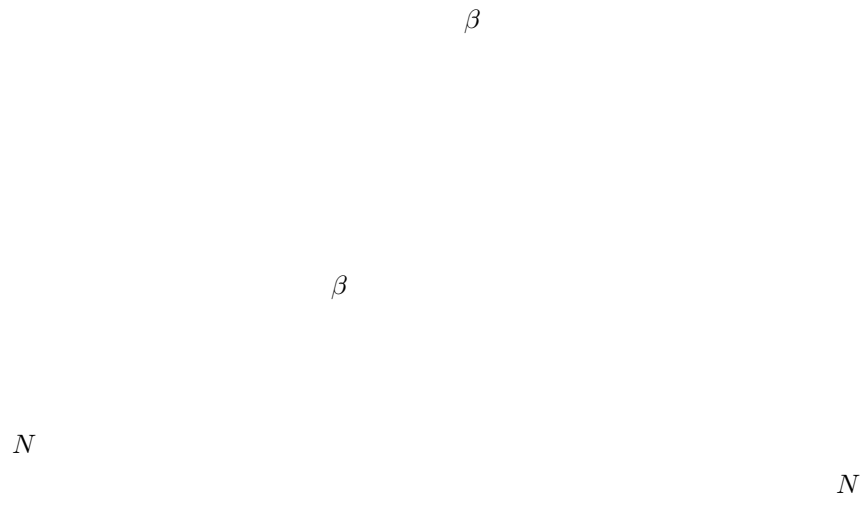

Figure 1: *The log-gamma family of densities with central mean* $< N >= \frac{1}{2}$ *as a surface and as a contour plot.*

```
2 & 1 & 1 \\
3 & 1 & 1 \\
4 & 1 & $\infty$ \\
5 & 1 & 1 \\
6 & 1 & 1 \\
7 & 28 & 1 \\
8 & 2 & 1 \\
9 & 8 & 1 \\
10 & 6 & 1 \\
11 & 992 & 1 \\
12 & 1 & 1 \\
13 & 3 & 1 \\
14 & 2 & 1 \\
15 & 16256 & 1 \\
\end{tabular}}
\caption{Numbers of distinct differentiable structures on real $n$-space
and $n$-spheres}
\label{diffstruc}
\end{center}
\end{table}
```

This allowed us to cross-reference the Table via:

```
~\ref{diffstruc}
```

5 Graphics

Figure **??** was created by calling in the two pdf graphics files `3dpdf.pdf` , `contpdf.pdf` placed together in the following `picture` environment inside a `figure` environment with a caption and label:

```
\begin{figure}
\begin{picture}(300,220)(0,0)
\put(210,100){$\beta$}
```

```
\put(400,25){$N$}
\put(260,200){$\beta$}
\put(90,40){$N$}
\end{picture}
\caption{{\em The log-gamma family of densities with central mean
$<N> \, = \frac{1}{2}$ as a surface and as a contour plot. }}
\label{pdf}
\end{figure}
```

References

[1] S-I. Amari. **Differential Geometrical Methods in Statistics**, Springer Lecture Notes in Statistics 28, Springer-Verlag, Berlin 1985.

[2] S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 398-412.

[3] G. Di Crescenzo and R. Ostrovsky. On concurrent zero-knowledge with pre-processing. In **Advances in Cryptology-CRYPTO '99** Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 485-502.

[4] C.T.J. Dodson and T. Poston. **Tensor Geometry**, Graduate Texts in Mathematics 130, Second edition, Springer-Verlag, New York, 1991. http://www.ma.umist.ac.uk/kd/tg.html

[5] O. Goldreich, A. Sahai and S. Vadham. Can Statistical Zero-Knowledge be made non-interactive? Or, on the relationship of SZK and NISZK. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 467-484.

[6] P. Kocher, J. Jaffe and B.Jun. Differential Power Analysis. In **Advances in Cryptology-CRYPTO '99**, Ed. M. Wiener, Lecture Notes in Computer Science 1666, Springer, Berlin 1999 pp 388-397.

[7] S.L. Lauritzen. Statistical Manifolds. In **Differential Geometry in Statistical Inference**, Institute of Mathematical Statistics Lecture Notes, Volume 10, Berkeley 1987, pp 163-218.