MODULATION FORENSICS FOR WIRELESS DIGITAL COMMUNICATIONS

W. Sabrina Lin and K. J. Ray Liu

ECE Dept., University of Maryland, College Park, MD 20742 USA
Email: {wylin, kjrliu}@eng.umd.edu

ABSTRACT

Modulation forensics is to detect the modulation type in wireless communications without any prior information. It finds both military and civilian applications such as surveillance and cognitive radio. It is a challenging task, especially in a non-cooperative environment, as no prior information on the incoming signal is available at the receiver. In this paper, we investigate the modulation forensics of linear digital modulations and space-time orthogonal code in slowly varying frequency-selective fading channels. With unknown channel vector, and phase distortion at the receive-side, we derive a composite test consisting second-moment nonlinearity and maximum likelihood test, and discuss the performance and forensic system confidence measure. It is shown that the proposed algorithm achieves almost perfect identification of the space-time coding, and high accuracy rate of modulation type detection.

Index Terms— Modulation forensics, security

1. INTRODUCTION

Within the past decades, the explosive development of wireless communication technologies facilitates the transmissions of all kinds of information over wireless channels: talking to each other, distributing multimedia, sharing private content, and military command and control, no matter where the receivers are. However, the broadcast nature of wireless channel also allows everyone in the network to listen to others' signal. From the national security point of view, any suspicious damaging activities should be under surveillance. Thus, it's crucial to develop a forensic scheme that is able to decode the information from the received signals without any prior information. The very first step of communication forensic detector is to determine which kind of modulation is in use.

Modulation forensics detector is not only useful to security or military purposes, but also to many other civilian applications. For example, in cognitive radios, detecting the modulation type of the current user help to identify whether the primary user is presented or not, yet facilitates spectrum sharing. The more accurate the modulation forensics detector is, the more efficient the cognitive radio.

In the literature, two categories of approaches have been adopted to tackle this problem: statistics-based pattern recognition approach, in which features are extracted from the received signal and their differences are used for decision -making [1, 2, 3]; and the other is likelihood-based approach, in which the likelihood function (LF) of the received signal is computed and a likelihood ratio test is used for detection [4, 5, 6, 7, 8].

The likelihood based method is shown to be asymptotically optimal in [4], and the theoretical performance bound is derived under the assumption that all communication parameters are known. Since the forensic detector is working blindly by listening to others' signals, the communication parameters are not available in such applications. Most of the prior works identify the digital modulation types in additive white Gaussian noise channel [5], and some more recent works move further to flat fading channel[8, 6, 7]. However, the more realistic frequency-selective fading channels for broadband wireless communications have not been addressed in prior works.

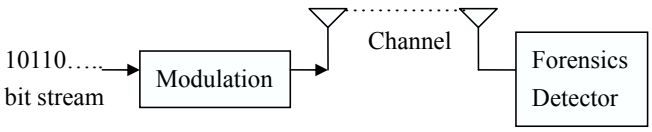

Fig. 1. Modulation Forensic System Model

In addition, most of the prior works only discuss under single input single output (SISO) system, but space-time coding [9] has been very widely used within the past decade to achieve transmit diversity in wireless communications. For forensic purpose, it's crucial to detect whether it is multiple input multiple output (MIMO) system, how many transmit antennas are used in the transmitter's side, and which space-time coding or modulation scheme is employed.

In this paper, we propose a SISO/MIMO modulation forensic detector in frequency-selective fading channel. In Section 2 the signal model and modulation forensic detector problem formulation are presented. The forensic detector methodology is proposed in Sections 3. Simulation results are discussed in Section 4, followed by conclusions in Section 5.

2. SYSTEM MODEL AND PROBLEM FORMULATION

Figure 1 shows the system model of the forensic detector: the original bit stream is modulated and gone through the fading channel. The input of the modulation forensic detector is the signal directly received from the receiver antenna.

In SISO system, the received baseband signal sequence at the output of the matched filter is expressed as

$$\mathbf{r} = \mathbf{C}_K(\mathbf{c}, \mathbf{s}^{(i)})e^{j\theta} + \mathbf{n}, i = 1, ...N_{mod} \quad (1)$$

where $\mathbf{r} = [r_1, r_2, ..., r_K]^T$ is the vector of samples at the output of equalizer, taken at the symbol rate, with K as the number of observed symbols, $\mathbf{s}^{(i)} = [s_1^{(i)}, s_2^{(i)}, ..., s_K^{(i)}]^T$ is the transmitted symbol sequence of ith modulation format, $\mathbf{n}$ is the estimated noise vector [10]. We model the fading channel as a M tap linear filter: $\mathbf{c} = [c_1, c_2, ..., c_M]^T$ is the channel amplitude vector, θ is the channel phase including the carrier phase offset, and N_{mod} is the number of possible SISO modulation type in our forensic detector. The AWGN noise components $\{n^k\}_{k=1}^K$ are zero-mean Gaussian distributed, with variance N. The sequence $\{s_k^{(i)}\}_{k=1}^K$ is independent and identically distributed, with values drawn from a finite

set specific to the ith modulation format, $i = 1, ..., N_{mod}$. $\mathbf{C}_K(\mathbf{c}, \mathbf{s})$ is the first K terms of the convolution of channel vector $\mathbf{c}$ and transmitted symbol vector $s^{(i)}$. In this work, linearly digitally modulated signals are considered.

If the transmitter is using multiple antenna and orthogonal space-time code, then

$$\mathbf{r}^{MIMO} = \sum_{l=1}^{q} \mathbf{C}_K(\mathbf{c}^l, \mathbf{x}^l) e^{j\theta^l} + n, \tag{2}$$

where q is the number of transmit antenna, $\mathbf{x}^l = [x_1^l, x_2^l, ..., x_K^l]$ is the transmitted symbol vector at antenna l based on the space-time coding matrix. $\mathbf{c}^l = [c_1^l, c_2^l, ..., c_M^l]$ is the channel amplitude vector, and θ^l is the phase distortion between transmit antenna l and the receive antenna. Thus, start from the baseband signal of one receive antenna of the modulation forensic detector, the first question is how to distinguish the MIMO system with the SISO one. And next, if there are multiple transmit antennas, which orthogonal space-time code is used? If the system is SISO, how to tell the modulation scheme?

3. FORENSIC DETECTOR

To remove the channel effect, the first step of the forensic detector is to perform SISO blind equalization [11]. Then, based on the equalized received baseband signal, in the following section, we'll discuss how the modulation forensic detector identify number of transmit antennas and the space-time codec.

3.1. MIMO/SISO Identification

After equalization, (1) becomes:

$$\mathbf{r}' = e^{j\theta}\mathbf{s}^{(i)} + \mathbf{n}' \tag{3}$$

and it's easy to show that (2) becomes:

$$\mathbf{r}^{MIMO'} = \mathbf{D}(c_e, \mathbf{r}^{MIMO}) = \sum_{l=1}^{q} \mathbf{C}_K(g_{(l)}\mathbf{x}^{(l)}) e^{j\theta^{(l)}} + n' \tag{4}$$

Where c_e is the estimated channel amplitude vector by the blind equalizer, $\mathbf{D}$ is the deconvolution operation, and every $g_{(l)}$, $1 \le l \le q$, is a filter satisfies:

$$\text{convolution}(c_e, g_{(l)}) = c^l \quad 1 \le l \le q \tag{5}$$

With perfect equalizer, $\mathbf{n}'$ is a Gaussian random vector.

To identify MIMO systems, we introduce the second moment test: let

$$M(d) = E[r_1'^2 r_{d+1}'^2] - E[r_1'^2]E[r_{d+1}'^2] \tag{6}$$

if the system is SISO, that is, r' as in (3), because every symbol is independent,

$$E[r_1'^2 r_{d+1}'^2] = E[r_1'^2]E[r_{d+1}'^2] \quad \forall d < K \tag{7}$$

, thus M(d) = 0 $\quad \forall d < K$.

If the transmitter side is using $p \times q$ space-time diagonal code, then M(d) $\neq 0$ $\forall 1 \le d < q$, and M(d) ≈ 0 , otherwise. To illustrate this, take the 2-by-2 orthogonal space-time code as an example:

$$C_2 = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix} \tag{8}$$

The second moment test M(1) is:

$$\begin{aligned} M(1) &= (g_{(1)}^2(0)s_1^2 e^{2j\theta^{(1)}} + g_{(2)}^2(0)s_2^2 e^{2j\theta^{(2)}} + \\ &\quad +2g_{(1)}(0)g_{(2)}(0)s_1 s_2 e^{j(\theta^{(1)}+\theta^{(2)})}) \times \\ &\quad (g_{(1)}^2(0)(s_2^2)^* e^{-2j\theta^{(2)}} + g_{(2)}^2(0)(s_1^2)^* e^{-2j\theta^{(1)}} \\ &\quad -2g_{(1)}(0)g_{(2)}(0)s_1^* s_2^* e^{-j(\theta^{(1)}+\theta^{(2)})}) \\ &\quad -(g_{(1)}^2(0)s_1^2 e^{2j\theta^{(1)}} + g_{(2)}^2(0)s_2^2 e^{2j\theta^{(2)}}) \times \\ &\quad (g_{(1)}^2(0)(s_2^2)^* e^{-2j\theta^{(2)}} + g_{(2)}^2(0)(s_1^2)^* e^{-2j\theta^{(1)}}) \\ &\quad +O(g_{(2)}, g_{(2)}, x) \\ &= -4g_{(1)}^2(0)g_{(2)}^2(0)|s_1|^2|s_2|^2 + O(g_{(2)}, g_{(2)}, x) \\ &\approx -4g_{(1)}^2(0)g_{(2)}^2(0)|s_1|^2|s_2|^2 \neq 0 \end{aligned} \tag{9}$$

Where $O(g_{(2)}, g_{(2)}, x)$ is the tail term corresponding to the imperfect channel amplitude estimation.

Thus, by performing the second-moment test, we can easily tell how many transmit antennas are used.

After determining the space domain codeword length, we need to determine the time domain codeword length, and since to this stage we know the number of transmit antennas, we can perform MIMO blind equalization [12] to improve our estimation of $\{M(d)\}_{d=1}^{q}$ in (6). To achieve full diversity and maintain equal energy for every symbol, given the space domain codeword length q, there are only a few possibilities of space-time code matrix and every matrix has unique formulation of $\{M(d)\}_{d=1}^{q}$. Thus, we construct a support vector machine (SVM) classifier using $\{M(d)\}_{d=1}^{q}$ calculated from the received signals r' as the input feature to determine the time domain codeword length and the space-time code matrix.

Once we have the space-time code matrix, we can decode the received baseband signals into symbol sequence $\mathbf{s}^{(i)}$, and perform the same modulation detection as SISO system in the following section.

3.2. SISO Modulation Detector

The SISO modulation forensic detector, with the likelihood-based approach, is formulated as a multiple composite hypothesis testing problem [13]. Under hypothesis H_i, meaning the ith modulation was transmitted,where $i = 1, ..., N_{mod}$, the likelihood function can be computed by estimating the unknown parameter θ. By assuming that the equalized received symbols are statistically independent, under hypothesis H_i ,the conditional likelihood function is given by

$$\begin{aligned} f(\mathbf{r}'|\{s_k^{(i)}\}_{k=1}^K, \theta) &= \prod_{k=1}^{K} \frac{1}{\pi N'} \exp\{-\frac{1}{N'}|r_k' - e^{j\theta}s_k^{(i)}|^2\} \\ &= \frac{1}{(\pi N')^K} \exp\{-\frac{1}{N'}\|\mathbf{r}' - e^{j\theta}\mathbf{s}^{(i)}\|^2\} \end{aligned} \tag{10}$$

the likelihood function is computed by averaging over the unknown signal constellation points $\{s_k^{(i)}\}_{k=1}^K$ and replacing the unknown phase distortion with its respective estimate. Thus, the likelihood function under the ith hypothesis can be written as

$$LF^{(i)}(\mathbf{r}') = E_{\{s_k^{(i)}\}_{k=1}^K}[f(\mathbf{r}', \widetilde{\theta}|\{s_k^{(i)}\}_{k=1}^K)] \tag{11}$$

where $E_{\{s_k^{(i)}\}_{k=1}^K}[\cdot]$ is the expectation with respect to the unknown transmitted symbol constellation points and $\widetilde{\theta}$ is the unknown phase distortion estimates under the ith hypothesis H_i.

The final decision of modulation scheme $\widetilde{i}$ is made based on maximum likelihood criteria, that is, $\widetilde{i}$ satisfies:

$$\widetilde{i} = \arg \max_{i=1,...,N_{mod}} LF^{(i)}(\mathbf{r}') \tag{12}$$

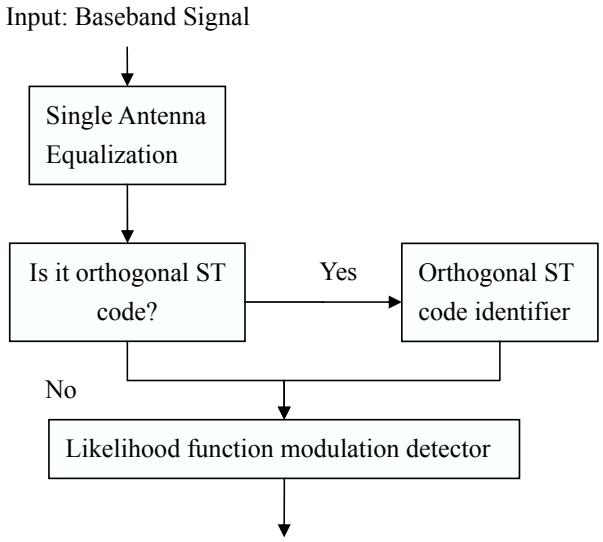

Fig. 2. Overall modulation forensic detector scheme

Since the likelihood function in (11) is computed by using maximum likelihood estimate of phase distortion, $\widetilde{\theta}$ should satisfies:

$$\frac{\partial f(\mathbf{r}'|\{s_k^{(i)}\}_{k=1}^{K},\theta)}{\partial\theta}\Big|_{\theta=\widetilde{\theta}^{(i)}}=0 \tag{13}$$

By solving (13), we show that

$$\widetilde{\theta}^{(i)}=-\frac{j}{2}\ln\left(\frac{\mathbf{s}^{(i)\mathbf{H}}\mathbf{r}}{\mathbf{r}^{\mathbf{H}}\mathbf{s}^{(i)}}\right) \tag{14}$$

3.3. Overall Forensic Detector Scheme

Figure 3.3 shows the overall methodology of the modulation forensic detector: upon receiving the baseband signal, first apply the single antenna blind equalization, and then identify whether space-time coding is presented as discussed in Section 3.1: If so, estimate the coding matrix and transform the received signal to transmitted symbols and then go through the modulation detector; if not, apply the modulation detector on the equalized signal directly.

The task of the forensic detector is not only to estimate the correct modulation scheme as precisely as possible, but also gives a confidence measure to every estimation. We define the detector's confidence **C** measure as follows:

$$\mathrm{C}=1-\frac{H(\mathbf{LF})}{\log_2 N_{mod}} \tag{15}$$

where

$$\mathbf{LF}=\frac{\{LF^{(1)},...,LF^{(N_{mod})}\}}{\sum_{i=1}^{N_{mod}}LF^{(i)}} \tag{16}$$

is the normalized likelihood vector of all the hypotheses. From the above analysis, when $LF^{(\widetilde{i})}$ is much larger than the other $LF^{(i)}$s, the vector **LF** has a smaller entropy $H(\mathbf{LF})$, which means one of the modulation type is much more likely than each other, thus we are more confident with the detection result. The lower the entropy

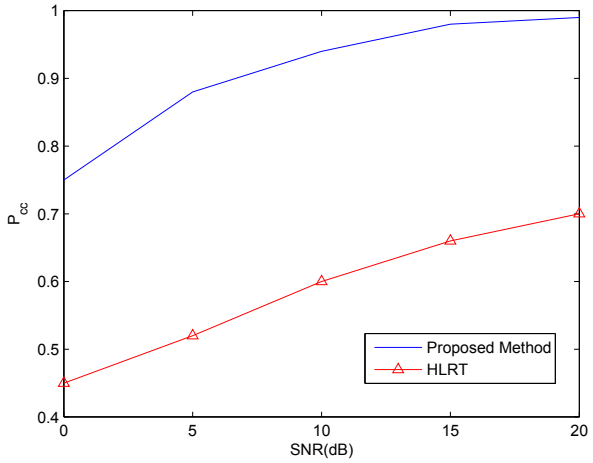

Fig. 3. Performance comparison of likelihood-based algorithms in frequency-selective Rayleigh fading, when discriminating BPSK, QPSK,and 8-PSK with K =60 symbols

$H(\mathbf{LF})$, the more confident the forensic detector is. Based on this idea, the confidence measure **C** is defined as 1-normalized entropy of $H(\mathbf{LF})$ as in (**??**).

4. SIMULATION RESULT

To compare the SISO modulation forensics detector detector's performance over frequency selective fading channel, besides our forensic detector, the performance of hybrid likelihood ratio test (HLRT) is also shown [4]. We consider the most commonly used digital modulations: BPSK, QPSK, 8-PSK and 16-QAM as candidate modulations. Without any loss of generality, normalized constellations are generated in simulations, i.e.,$E[|s_k^{(i)}|^2]$=1, thus, the SNR is changed by varying the noise power only. The pulse shape is rectangular, of unit amplitude and duration T seconds. The symbol period T is set to one ms. The average probability of correct classification is used to evaluate the performance. This is defined as

$$P_{cc}=\frac{\sum_{i=1}^{N_{mod}}P_c^{(i|i)}}{N_{mod}} \tag{17}$$

where $P_c^{(i|i)}$ is the conditional probability of the event that the ith modulation is received when indeed the ith modulation was originally transmitted. The number of symbols used to calculate $P_c^{(i|i)}$ is 30 and another 30 symbols are used for blind equalization. The channel is frequency-selective with Rayleigh fading.

Figure 3 shows the modulation detector's performance under SISO systems and frequency selective Rayleigh fading channel. It's clear that our method is 20 percent outperform HLRT and can achieve over 95 percent accuracy rate in high SNR with only 60 symbols. This is because HLRT has the assumption of AWGN channel, which degrades the performance a lot in selective fading channel, although HLRT has very high accuracy rate in AWGN channel.

The performance of overall modulation forensic detector as discussed in Section 3.3 is in Figure 4. Since there's no prior work on MIMO forensic detector, Figure 4 only shows our detection accuracy and Figure 5 plots the output system confidence measure . We test

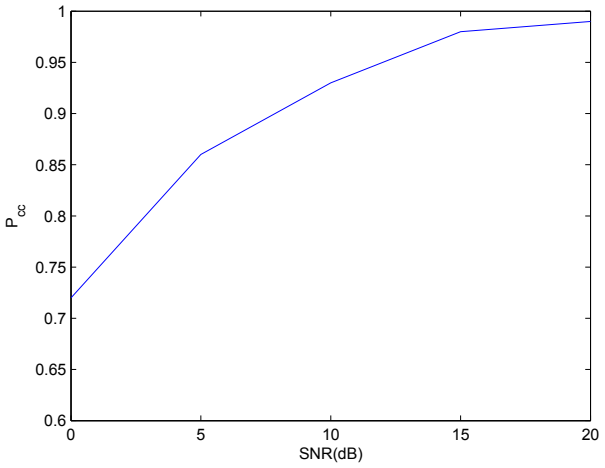

Fig. 4. Overall performance of the modulation forensics detector including BPSK, QPSK, 8PSK, and diagonal space-time code C_2, $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$ with K = 100 symbols

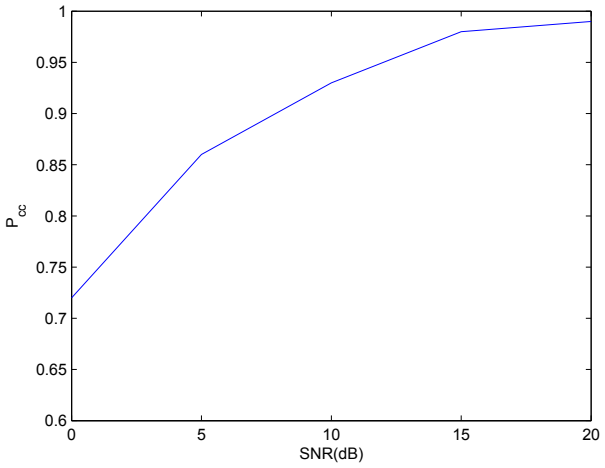

Fig. 5. Output Confidence Measure of the modulation forensics detector including BPSK, QPSK, 8PSK, and diagonal space-time code C_2, $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$ with K = 100 symbols

over four commonly used orthogonal space-time codes:C_2, $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$, which maintain same transmit power. We need a little bit more symbols to determine the space-time code scheme, so here we show the result of K = 100 symbols.

Comparing Figure 4 and Figure 3, one can find that there is just a 2 percent performance derations by including the MIMO system identification, which means our space-time matrix estimation method has similar performance with the optimal one. And, the performance of MIMO system identification rarely degrades with SNR, because our method is based on the transmit symbols' orthogonality, which is independent of SNR. Also, the performances in high SNR begin the same also implies that increasing the number of test symbols from 60 to 100 doesn't help much in detection, which means our likelihood-based test can work well with short symbol length 60. This feature is very important for forensics purpose, since the shorter the delay, the more the information.

Although the modulation forensics detector makes some error in low SNR (SNR$<$10 dB), the corresponding output system confidence measure is also low as in Figure 5. Which means the modulation forensic detector still works well in low SNR: the forensic detector is very uncertain about the answer when making errors.

5. CONCLUSION

In this paper, we proposed a composite likelihood ratio and second moment test for MIMO/SISO digital linear modulation forensics detection in frequency-selective fading channels, with unknown channel amplitude vector and phase distortion. The overall modulation forensics detector achieves very high detection accuracy, which approaches to 1 in SNR$>$15 dB, in fading channel with only 60 symbols. And the simulation results shows that the proposed space-time orthogonal coding identification base on second-moment nonlinearity test is nearly perfect.

6. REFERENCES

[1] C. M. Spooner, "On the utility of sixth-order cyclic cumulants for rf signal classification," *in Proc. IEEE ASILOMAR*, pp. 890–897, 2001.

[2] A. Swami and B. M. Sadler, "Hierarchical digital modulation classification using cumulants," *IEEE Transaction on Communication*, vol. 48, pp. 416–429, 2000.

[3] W. Dai, Y. Wang, and J. Wang, "Joint power estimation and modulation classification using second- and higher statistics," *in Proc. IEEE WCNC*, pp. 155–158, 2002.

[4] W. Wei and J. M. Mendel, "Maximum-likelihood classification for digital amplitude-phase modulations," *IEEE Transaction on Communication*, vol. 48, pp. 189–193, 2000.

[5] A. Polydoros and K. Kim, "On the detection and classification of quadrature digital modulations in broad-band noise," *IEEE Transaction on Communication*, vol. 38, pp. 1199–1211, 1990.

[6] O. A. Dobre, J. Zarzoso, Y. Bar-Ness, and W. Su, "On the classification of linearly modulated signals in fading channels," *in Proc. Conference on Information Sciences and Systems (CISS)*, 2004.

[7] A. Abdi, O. A. Dobre, R. Chauchy, Y. Bar-Ness, and W. Su, "Modulation classification in fading channels using antenna arrays," *in Proceeding of IEEE MILCOM*, pp. 211–217, 2004.

[8] O. A. Dobre and F. Hameed, "Likelihood-based algorithms for linear digital modulation classification in fading channels," *Proc. IEEE CCECE, Ottawa, Canada.*, 2006.

[9] S.M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451V1458, 1998.

[10] R. Matzner and F. Engleberger, "An snr estimation algorithm using fourth-order moments," *in Proc. IEEE Int. Symp. Information Theory*, p. 199, June 1994.

[11] B. Sampath, Ray Liu K, J, and Y. Goeffrey Li, "Error correcting least-squares subspace algorithm for blind identification and equalization," *Signal Processing*, vol. 8, no. 10, pp. 2069–2087, 2001.

[12] B. Sampath, K.J. Ray Liu, and Y. Goeffrey Li, "Deterministic blind subspace mimo equalization," *EURASIP Journal On Applied Signal Processing*, , no. 5, pp. 538–551, 2002.

[13] H. V. Poor, *An Introducton to Signal Detection and Estimation*, Springer Verlag, 2nd edition, 1999.