

Synchronization of Pseudo-Random Signals by Forward-Only Message Passing with Application to Electronic Circuits

Benjamin Vigoda, Justin Dauwels, Matthias Frey, Neil Gershenfeld,
Tobias Koch, Hans-Andrea Loeliger, and Patrick Merkli

Abstract—It has been observed that a linear-feedback shift-register (LFSR) sequence can be synchronized by feeding the modulated sequence into a “soft” (or “analog”) version of the LFSR. In this paper, the “soft LFSR” is derived as forward-only message passing in the corresponding factor graph. A continuous-time analog (suitable for realization as a clockless electronic circuit) is then given of both the LFSR and the soft LFSR. A connection is thus established between statistical state estimation and the phenomenon of entrainment of dynamical systems, which opens the prospect of deriving dynamical systems (such as electronic circuits) with strong entrainment capabilities from more powerful message passing algorithms.

Keywords—LFSR, synchronization, factor graphs, message passing, nonlinear filtering, circuits, dynamical systems, entrainment.

1 Introduction

Pseudo-random signals play an important role in spread-spectrum communications [1], [2] and in various measurement systems. In such systems, the synchronization of pseudo-random signals is a problem of significant interest. The standard solution to this problem is based on correlating the incoming signal with (a segment of) the pseudo-random signal, which leads to a long acquisition time if the period of the signal is large.

B. Vigoda was with the MIT Media Lab, MIT, Cambridge, MA, 02139. He is now with the Mitsubishi Electric Research Lab, 201 Broadway, Cambridge, MA, 02139. Email: vigoda@media.mit.edu.

N. Gershenfeld is with the MIT Center for Bits and Atoms, MIT, Cambridge, MA, 02139. Email: neilg@cba.mit.edu.

J. Dauwels, M. Frey, T. Koch, and H.-A. Loeliger are with the Dept. of Information Technology and Electrical Engineering, ETH Zurich, CH-8092 Zürich, Switzerland. Email: {dauwels, frey, tkoch, loeliger}@isi.ee.ethz.ch.

P. Merkli was with the Dept. of Information Technology and Electrical Engineering, ETH Zurich, CH-8092 Zürich, Switzerland. He is now with Sensirion AG, Zurich, Switzerland. Email: patrick.merkli@sensirion.com.

B. Vigoda and N. Gershenfeld wish to acknowledge the support by NSF grant CCR-0122419.

J. Dauwels wishes to acknowledge the support by Swiss NF grant 200021-101955.

Perhaps the most popular class of pseudo-random signals are generated by linear-feedback shift registers (LFSRs). Both Gershenfeld and Grinstein [3] and Yang and Hanzo [4], [5] observed that LFSR sequences can be synchronized by means of a “soft” or “analog” LFSR. The approach of [3] is system theoretic: the soft LFSR is a dynamical system with entrainment capabilities (cf. [6], [7], [8]) obtained by embedding the discrete state space of the LFSR into a continuous state space. By contrast, the (better) soft LFSR of [4], [5], which was independently obtained also in [9], is derived from statistical estimation; it achieves quick synchronization—e.g., after 150 samples at 0 dB for an LFSR with a period of $2^{15} - 1$ samples—at very low computational cost. Related algorithms, some of them more complex and more powerful, were presented in [9], [10], [11], [12], [13].

In this paper, we connect the dynamical systems view of [3] with the statistical view of [4], [5], both in discrete time and in continuous time. First, we derive the soft LFSR of [4], [5] as forward-only message passing in the corresponding factor graph. We then propose a new continuous-time analog of both the LFSR and the soft LFSR, both suitable for realization as electronic circuits. We actually implemented one such circuit, and we report some measurements. It is thus demonstrated that continuous-time dynamical systems (such as clockless electronic circuits) with good entrainment properties can be derived from message passing algorithms for statistical state estimation. Such systems/circuits may have substantial advantages in terms of speed and/or power consumption over digital implementations in some applications, and they may enable entirely new applications. However, such applications are outside the scope of this paper.

This paper is structured as follows. We begin by stating the discrete-time problem in Section 2. In Section 3, we review maximum-likelihood estimation and its interpretation as forward-only message passing in a cycle-free factor graph. In Section 4, we obtain the soft LFSR as forward-only message passing through another factor graph, and we present some simulation results. A continuous-time analog of the (discrete-time) LFSR is proposed in Section 5. The corresponding continuous-time analog of the soft LFSR and its realization as an electronic circuit are described in Section 6. Some measurements of this circuit are reported in Section 7, and some conclusions are offered in Section 8. Some details of alternative versions of the soft LFSR (sum-product, max-product, and Gershenfeld-Grinstein) are given in the Appendix.

2 Noisy LFSR Sequences

For fixed integers ℓ and m satisfying $1 \leq \ell < m$, let

$$X \triangleq X_{-m+1}, \dots, X_{-1}, X_0, X_1, X_2, \dots \quad (1)$$

be a binary sequence satisfying the recursion

$$X_k = X_{k-\ell} \oplus X_{k-m} \quad (2)$$

for $k = 1, 2, 3, \dots$, where “ \oplus ” denotes addition modulo 2. Any such sequence will be called a LFSR (linear-feedback shift register) sequence. For $k \geq 0$, the m -tuple $[X]_k \triangleq$

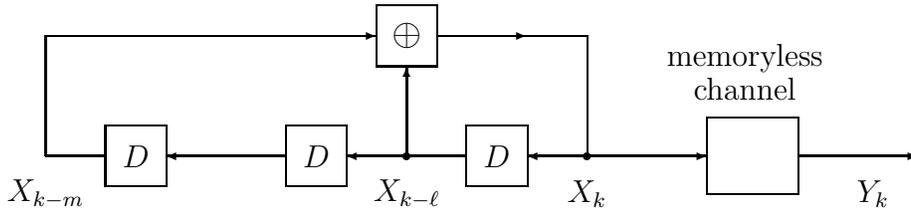


Figure 1: LFSR sequence observed via a noisy channel.

$(X_{k-m+1}, \dots, X_{k-1}, X_k)$ will be called the *state* of X at time k . The sequence X_1, X_2, \dots is observed via a memoryless channel with transition probabilities $p(y_k|x_k)$. The situation is illustrated in Fig. 1 for $\ell = 1$ and $m = 3$; the boxes labeled “D” are unit-delay cells.

Note that the restriction to two right-hand terms (“taps”) in (2) is made only to keep the notation as simple as possible; all results of this paper are easily generalized to more taps. We also remark that, in most applications (and in our examples), LFSR sequences with the maximal period of $2^m - 1$ are preferred, but this condition plays no essential role in this paper.

From the received sequence Y_1, Y_2, \dots, Y_n , we wish to estimate the state $[X]_n$ of the transmitted sequence. The computation of the maximum-likelihood (ML) estimate is straightforward and well known [1]; however, the complexity of this computation is proportional to $n2^m$, which makes it impractical unless m is small.

In the examples, we will assume that the channel is defined by

$$Y_k = \tilde{X}_k + Z_k \quad (3)$$

with

$$\tilde{X}_k \triangleq \begin{cases} 1, & \text{if } X_k = 0 \\ -1, & \text{if } X_k = 1 \end{cases} \quad (4)$$

(i.e., binary antipodal signaling) and where $Z = Z_1, Z_2, \dots$ is white Gaussian noise (i.e., independent zero-mean Gaussian random variables) with variance σ^2 .

3 ML Estimation, Trellis, and Factor Graphs

Let us recall some basic facts. First, we note that the mapping $x \mapsto [x]_k$ (from sequences to states) is invertible for any $k \geq 0$: from the forward recursion (2) and the backward recursion $X_{k-m} = X_k \oplus X_{k-\ell}$, the complete sequence x is determined by its state at any time k .

Second, we consider the maximum-likelihood (ML) estimate of $[X]_n$. Using the notation $y^n \triangleq (y_1, \dots, y_n)$ and $x^n \triangleq (x_{-m+1}, \dots, x_n)$, the ML estimate of $[X]_n$ is the maximum

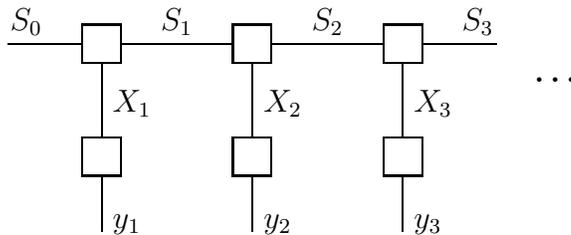


Figure 2: Factor graph (Forney-style) corresponding to the trellis of the system in Fig. 1.

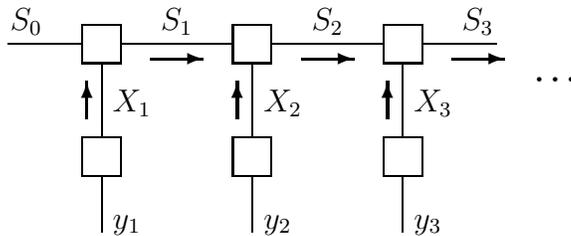


Figure 3: Forward-only message passing through the factor graph of Fig. 2.

(over all possible states $[x]_n$) of the likelihood function

$$p(y^n | [x]_n) = p(y^n | x^n) \quad (5)$$

$$= \prod_{k=1}^n p(y_k | x_k). \quad (6)$$

For the channel (3), maximizing (6) amounts to maximizing the correlation between \tilde{x}^n and y^n .

Third, we note that the computation of (6) may be viewed as the forward recursion of the BCJR algorithm [14] through the trellis of the system or—equivalently—as forward-only message passing through the corresponding factor graph. Let us consider this more closely. Instead of factor graphs as in [15], we will use Forney-style factor graphs as in [16], where edges (or half-edges) represent variables and nodes (boxes) represent factors. A (Forney-style) factor graph of our system is shown in Fig. 2. (Add a circle on each edge to obtain a factor graph as in [15]). As in [16], we use capital letters for unknown variables and small letters for known (observed) variables. The nodes in the top row of Fig. 2 represent $\{0, 1\}$ -valued functions $J(s_{k-1}, x_k, s_k)$ that indicate the allowed combinations of old state $s_{k-1} = [x]_{k-1}$, output symbol x_k , and new state $s_k = [x]_k$. The nodes in the bottom row of Fig. 2 represent the channel transition probabilities $p(y_k | x_k)$. As a whole, the factor graph of Fig. 2 represents the function

$$p(y^n | x^n) J(x^n, s^n) = \prod_{k=1}^n J(s_{k-1}, x_k, s_k) p(y_k | x_k) \quad (7)$$

(defined for arbitrary binary sequences x^n), where $J(x^n, s^n) \triangleq \prod_{k=1}^n J(s_{k-1}, x_k, s_k)$ is the indicator function of valid LFSR sequences, which may also be viewed as a uniform prior over all valid x^n .

It then follows from basic factor graph theory [15], [16] that the a posteriori probability distribution over $S_n = [X]_n$ (and thus the MAP / ML estimate of S_n) is obtained from forward-only sum-product message passing as illustrated in Fig. 3. Since the trellis has no merging paths, the sum-product rule for the computation of messages reduces to a product-only rule and coincides with the max-product rule. By taking logarithms, the product-only rule becomes a sum-only rule; for the channel (3), this amounts to a recursive computation of the correlation between \tilde{x}^n and y^n .

4 The Soft LFSR

Another factor graph for our system is shown (for $\ell = 1$ and $m = 3$) in Fig. 4. This factor graph represents the function

$$p(y^n|x^n)J(x^n) = \prod_{k=1}^n \delta[x_k \oplus x_{k-\ell} \oplus x_{k-m}]p(y_k|x_k), \quad (8)$$

where $\delta[\cdot]$ is the Kronecker delta and where $J(x^n) = \prod_{k=1}^n \delta[x_k \oplus x_{k-\ell} \oplus x_{k-m}]$ is the indicator function for valid LFSR sequences according to (2).

As this factor graph has cycles, the standard sum-product and max-product algorithms become iterative algorithms. Such algorithms were investigated in [12] and [13]. In this paper, however, we stick to (non-iterative) forward-only message passing. Since (full-state) forward-only message passing is optimal in Fig. 3, there is hope that (scalar) forward-only message passing in Fig. 4 might do well also. In any case, forward-only message passing in Fig. 4 amounts to a simple recursion, which may be interpreted as running the received sequence Y through the “soft LFSR” circuit of Fig. 5. The quantities $\mu_{A,k}$, $\mu_{B,k}$, and μ_k in Fig. 5 are the messages indicated in Fig. 4. Note that the same message μ_k is sent along two edges out of the equality check node corresponding to X_k .

The computation of these messages (as indicated in Fig. 5) is a standard application of the sum-product or max-product rules [16]. Each message represents “pseudo-probabilities” $\tilde{p}(0)$ and $\tilde{p}(1)$, e.g., in the form $\tilde{p}(0)/\tilde{p}(1)$ or $\tilde{p}(0) - \tilde{p}(1)$. For the latter representation, the explicit sum-product update rules are as follows:

Initialization: $\mu_k = 0$ for $k = -m + 1, -m + 2, \dots, 0$.

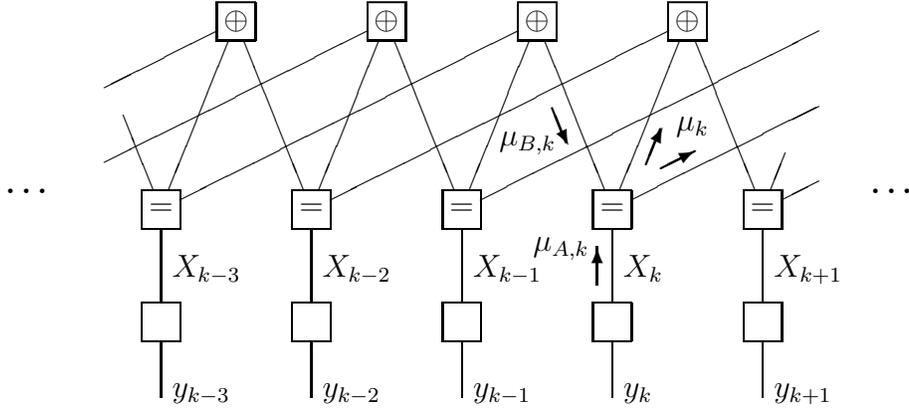


Figure 4: Factor graph corresponding directly to Fig. 1.

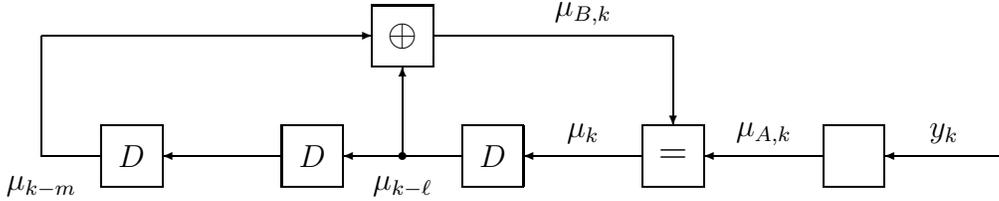


Figure 5: Computation of messages in Fig. 4 by a “soft LFSR”.

Recursion (for $k = 1, 2, 3, \dots$):

$$\mu_{A,k} = \frac{p(y_k|x_k = 0) - p(y_k|x_k = 1)}{p(y_k|x_k = 0) + p(y_k|x_k = 1)} \quad (9)$$

$$\text{for AWGN} \quad \mu_{A,k} = \frac{\exp(2y_k/\sigma^2) - 1}{\exp(2y_k/\sigma^2) + 1} \quad (10)$$

$$\mu_{B,k} = \mu_{k-\ell} \cdot \mu_{k-m} \quad (11)$$

$$\mu_k = \frac{\mu_{A,k} + \mu_{B,k}}{1 + \mu_{A,k} \cdot \mu_{B,k}} \quad (12)$$

Equation (9) holds for a general memoryless channel while (10) is the specialization to the channel specified at the end of Section 1. At any given time k , an estimate of X_k is obtained as

$$\hat{X}_k \triangleq \begin{cases} 0, & \text{if } \mu_k \geq 0 \\ 1, & \text{if } \mu_k < 0 \end{cases} \quad (13)$$

and $[\hat{X}]_k = (\hat{X}_{k-m+1}, \dots, \hat{X}_{k-1}, \hat{X}_k)$ is an estimate of the state $[X]_k$.

The sum-product update rules for the case where the messages represent the ratio $\tilde{p}(0)/\tilde{p}(1)$ are given in the appendix together with the max-product rules and the analog LFSR of [3].

Simulation results for maximum-length LFSR sequences with memory $m = 15$ and $m = 31$ are given in Figures 6–8. All these figures show plots of the probability of synchronization

$$P_{\text{synch}}(k) \triangleq P\left([\hat{X}]_k = [X]_k\right) \quad (14)$$

either vs. the time index k or vs. the signal-to-noise ratio $1/\sigma^2$ where σ^2 is the noise variance.

As is obvious from these plots (and from similar plots in [4], [5], [9]) the soft LFSR quickly achieves synchronization for sufficiently low noise power (up to about 0 dB) but fails for high noise power. It is remarkable that the max-product algorithm gives better performance than the sum-product algorithm, but the difference is small.

We also note that better performance can be achieved both with more complex forward-only message passing [9], [10] and with iterative message passing, cf. [12], [13].

5 A Continuous-Time Pseudo-Random Generator

We now proceed to an analog of Figures 1 and 5 in continuous time. Our proposal for a continuous-time analog of Fig. 1 is shown in Fig. 9. The signal $X(t)$ in Fig. 9 takes values in the set $\{+1, -1\}$. The multiplier in Fig. 9 corresponds to the mod-2 addition in Fig. 1.

How should we translate the delay cells in Fig. 1 to continuous time? An obvious approach would be to simply translate them into continuous-time delay cells. However, ideal continuous-time delay cells cannot be realized by real circuits (except perhaps in optics); even a delay line (e.g., a piece of wire) has a low-pass characteristic.

We therefore choose to replace the discrete-time delay cells of Fig. 1 by low-pass filters with transfer functions $H_1(s)$ and $H_2(s)$ as shown in Fig. 9. Since the output signal of such filters is not restricted to $\{+1, -1\}$, we introduce threshold elements between the filter outputs and the multiplier, which reduce the filtered signals to their sign (+1 or -1). These threshold elements have no counterpart in Fig. 1 (and will create a small problem in the receiver).

The memoryless channel in Fig. 1 is translated into the additive white Gaussian channel shown in Fig. 9.

The type of signal $X(t)$ generated by the circuit of Fig. 9 is illustrated in Fig. 10 (top). From our simulations, it appears that the signal $X(t)$ is generically periodic. The actual signal depends, of course, on the two filters. In our examples, the first filter (with transfer function $H_1(s)$) is a 5-th order Butterworth filter with -3 dB frequency 1.6 kHz, and the second filter (with transfer function $H_2(s)$) is a cascade of 6 such filters. With these filters, the circuit of Fig. 9 is a dynamical system with a 35-dimensional state space. The resulting signal $X(t)$ is periodic with a period of 34 ms, 10 ms of which are shown in Fig. 10 (top).

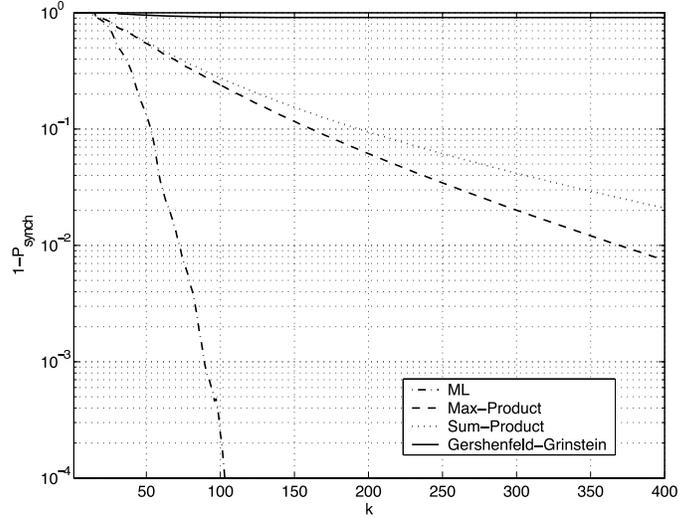


Figure 6: $1 - P_{\text{sync}}(k)$ for the LFSR with $m = 15$ ($\ell = 1$) at $\text{SNR} = 0$ dB. Algorithms (in the order of increasing performance): G.-G. soft LFSR [3]; sum-product soft LFSR; max-product soft LFSR; maximum likelihood (ML).

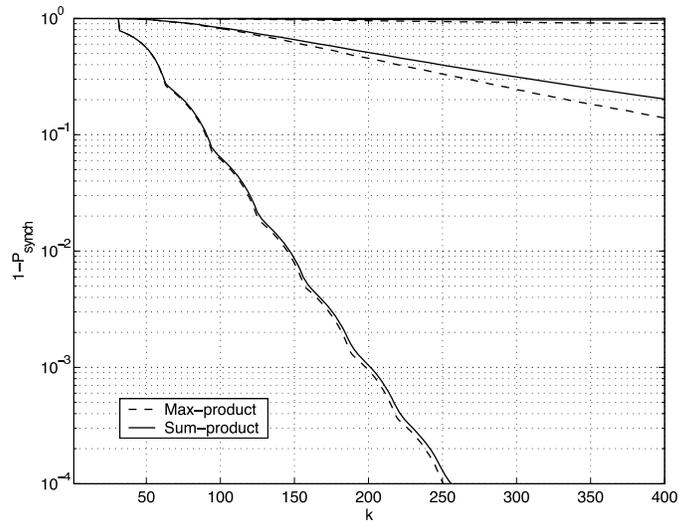


Figure 7: $1 - P_{\text{sync}}(k)$ for the LFSR with $m = 31$ ($\ell = 3$) for three different signal-to-noise ratios: $\text{SNR} = -2.92$ dB ($\sigma = 1.4$), $\text{SNR} = 0$ dB ($\sigma = 0$), and $\text{SNR} = 4.44$ dB ($\sigma = 0.6$). Algorithms: max-product soft LFSR and sum-product soft LFSR.

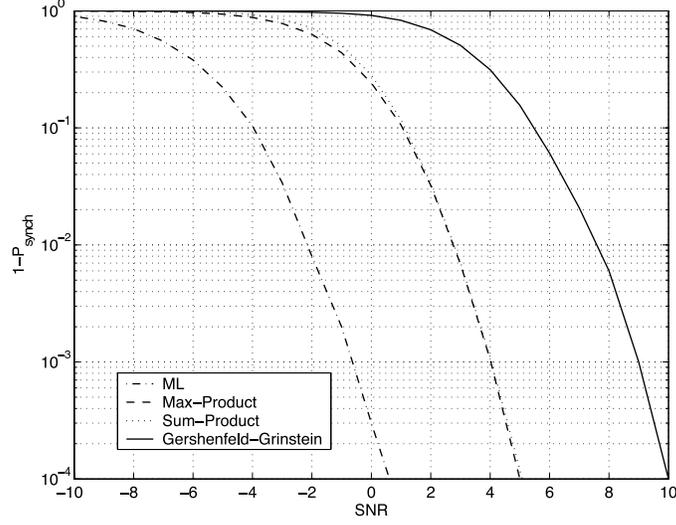


Figure 8: $1 - P_{\text{sync}}(k = 100)$ vs. SNR for the LFSR with $m = 15$ ($\ell = 1$). Algorithms (in the order of increasing performance): G.-G. soft LFSR [3]; sum-product soft LFSR; max-product soft LFSR; maximum likelihood (ML).

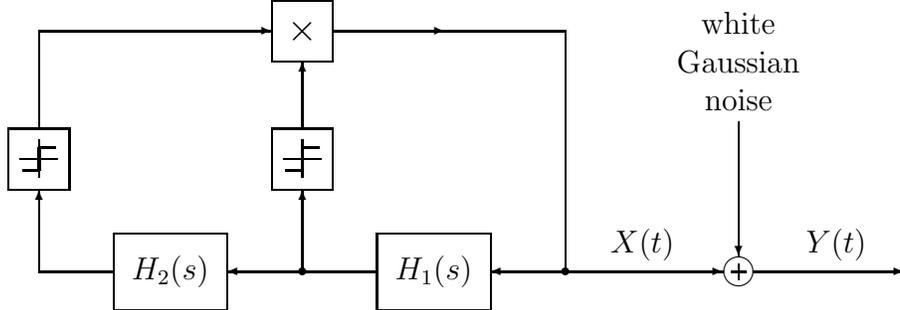


Figure 9: Continuous-time analog to Fig. 1 with low-pass filters instead of delay cells.

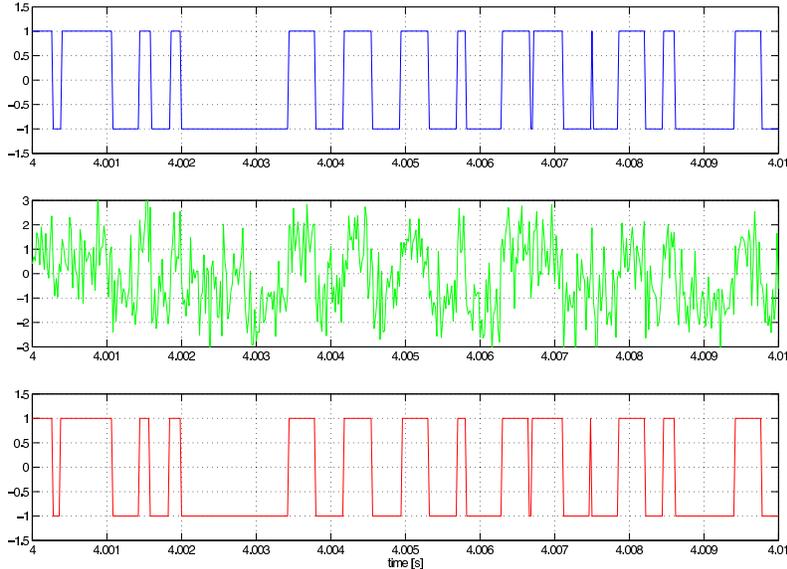


Figure 10: Top: example of pseudo-random signal $X(t)$ generated by the circuit of Fig. 9. Middle: noisy signal $Y(t)$ as in Fig. 9 at SNR = 0 dB. Bottom: measured output signal $\hat{X}(t)$ of the circuit of Fig. 11 fed with $Y(t)$.

It should be emphasized that, at present, we do not have a theory of such circuits and we cannot predict the period of the generated sequence $X(t)$. However, our simulation experiments (e.g., in [17]) suggest that a long period—“long” meaning many zero-crossings—requires a high-dimensional state space.

6 A Circuit that Locks onto the Pseudo-Random Signal

A continuous-time analog to the soft LFSR of Fig. 5 matched to the pseudo-random generator of Fig. 9 is shown in Fig. 11. The linear filters $H_1(s)$ and $H_2(s)$ in Fig. 11 are identical to those in Fig. 9. All signals in Fig. 11 should be viewed as approximations of *expectations* of the corresponding signals in Fig. 9 (conditioned on the previous observations). Note that, for $\{+1, -1\}$ valued signals, the mean coincides with the difference $\tilde{p}(+1) - \tilde{p}(-1)$. It follows that the multiplier ③ in Fig. 11 computes (the continuous-time analog of) the message $\mu_{A,k}(t)$ according to (11); the box ④ in Fig. 11 computes (the continuous-time analog of) the message μ_k according to (12); and the box ⑤ computes (the continuous-time analog of) the message $\mu_{A,k}$ according to (10). All these computations can be done by simple transistor circuits as described in [18], [19], [20] (where the pseudo-probabilities $\tilde{p}(+1)$ and $\tilde{p}(-1)$ are represented by a pair of currents).

Consider next the filtered signals. Let $S_1(t)$ denote the output signal of the filter

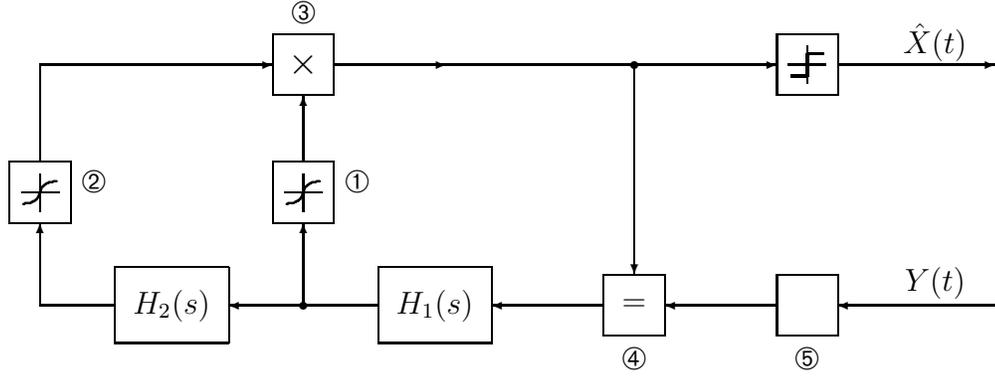


Figure 11: Continuous-time analog of Fig. 5.

$H_1(s)$ in Fig. 9 and let $h_1(t)$ be the impulse response of that filter (i.e., the inverse Laplace transform of $H_1(s)$). We thus have

$$S_1(t) = \int_{-\infty}^{\infty} h_1(\tau) X(t - \tau) d\tau \quad (15)$$

and

$$\mathbb{E}[S_1(t)] = \int_{-\infty}^{\infty} h_1(\tau) \mathbb{E}[X(t - \tau)] d\tau \quad (16)$$

where the expectation is a (time dependent) ensemble average based on the (time dependent) pseudo-probabilities $\tilde{p}(+1)$ and $\tilde{p}(-1)$. It follows that the output of the filter $H_1(s)$ in Fig. 11—which is given by the right-hand side of (16)—is the expected value of $S_1(t)$. In other words, *all* signals in Fig. 11 may be viewed as (approximations of) expectations of the corresponding signals in Fig. 9.

So far, all computations have been locally exact in the same sense as in the discrete-time case (i.e., ignoring cycles in the factor graph). This fails, however, for the threshold elements in Fig. 9: the (instantaneous) expectation of the output signal of such a threshold element is not determined by the (instantaneous) expectation of its input signal. At this point, however, practical considerations strongly suggest to implement the boxes ① and ② by the circuit of Fig. 12. This circuit accepts as input a voltage and produces as output two currents I_+ and I_- proportional to $\tilde{p}(+1)$ and $\tilde{p}(-1)$, respectively.

This same circuit is also used to implement the box ⑤ *exactly* (where the amplification α depends on the SNR and on the temperature). As an implementation of ① and ②, the circuit is an approximation; it would be exact (for the correct choice of α) if the distribution of the filtered signals—more precisely, the full sum-product message at the input of the soft-threshold elements—would be the logistic distribution

$$f(x) = \frac{1}{\beta \left(e^{\frac{x-\mu}{2\beta}} + e^{-\frac{x-\mu}{2\beta}} \right)^2} \quad (17)$$

with mean μ and variance $\pi\beta/\sqrt{3}$ [21, Appendix E]. In our experiments, the amplification α of these circuits was manually adjusted for the best performance.

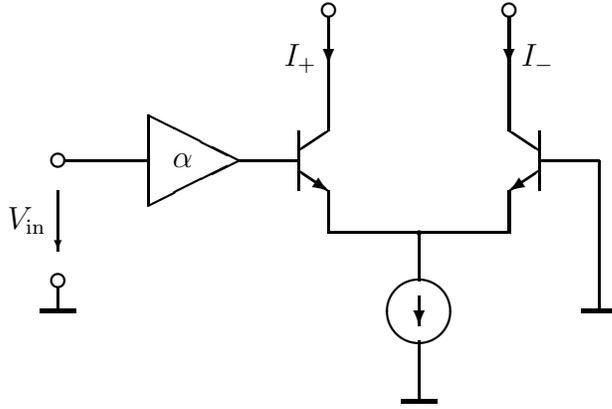


Figure 12: Differential transistor pair used for blocks ①, ②, and ⑤.

7 Some Measurements

Simulation results of analog circuits are often subject to doubt concerning their robustness with respect to nonidealities. We therefore built the system of Fig. 11 as an actual (clockless) electronic circuit with discrete components. The filters were realized as active RC filters with integrated operational amplifiers.

For the measurements, the clean signal $X(t)$ as well as the noisy signal $Y(t)$ were created by *simulating* the circuit of Fig. 9 on a (digital) computer; the noisy signal $Y(t)$ was then passed as input to the electronic realization of Fig. 11. A typical measured output signal $\hat{X}(t)$ is shown in Fig. 10 (bottom).

Some measurements of this system are given in Figures 13–15. For the measurements of Figures 13 and 14, the signal $Y(t)$ is replaced by a constant signal with value -1 for $t < 0$. Both figures show the squared error (SE) $(\hat{X}(t) - X(t))^2$ averaged, first, over a sliding window and then, over a number of experiments. Fig. 13 shows the SE (averaged over 10ms and over 5 experiments) vs. the time t ; Fig. 14 shows the SE (averaged over 1s and over 5 experiments) vs. the SNR at time $t = 4$ s (which is the steady state). Note that the receiver achieves good synchronization for an SNR down to about 0 dB. Not surprisingly, a signal with a longer period (top in Fig. 14) is more difficult to synchronize than a signal with a shorter period (bottom in Fig. 14).

It is instructive to observe what happens when the input to the receiving circuit is switched off for a while as illustrated in Fig. 15. Before the interruption, the receiver is synchronized. The signal $Y(t)$ is then masked (i.e., overwritten by zero) for 20 ms. During the interruption, $X(t)$ and $\hat{X}(t)$ drift apart and the averaged SE increases. The figure shows the signals $X(t)$ and $\hat{X}(t)$ around the critical moment when $Y(t)$ is switched on again.

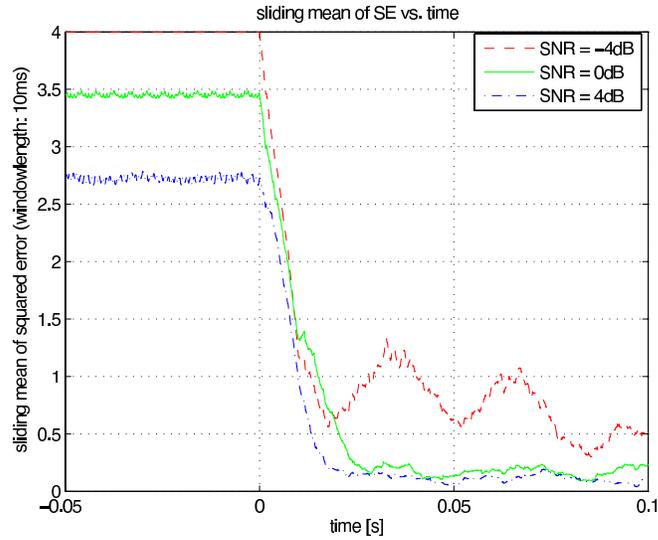


Figure 13: Average squared error vs. time after switching the transmission on.

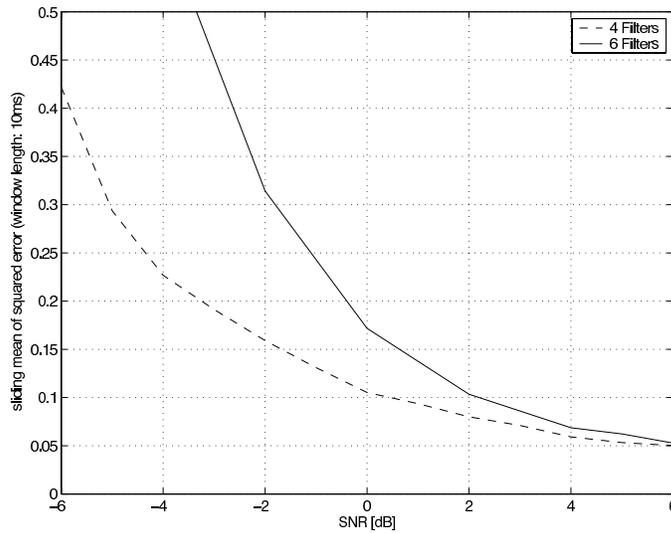


Figure 14: Average squared error in steady state vs. SNR. Dashed curve: pseudo-random signal with shorter period (7 ms instead of 34 ms, achieved with $H_2(s) = H_1(s)^4$ instead of $H_2(s) = H_1(s)^6$).

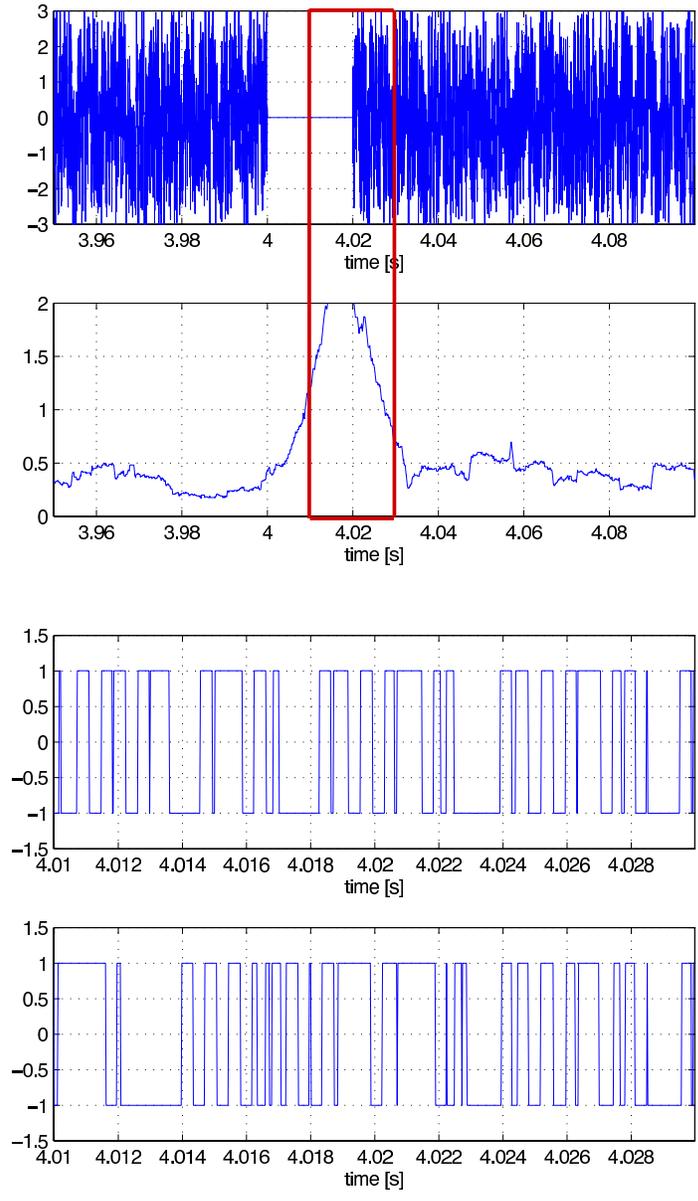


Figure 15: Resynchronization example with modified $Y(t)$ (top), sliding-window squared error (2nd from top), $X(t)$ (2nd from bottom), and $\hat{X}(t)$ (bottom) at SNR = 0 dB. The plots of $X(t)$ and $\hat{X}(t)$ are zoomed to the interval marked by the dashed lines.

8 Concluding Remarks

Gershenfeld and Grinstein demonstrated the synchronization of LFSR sequences (both in discrete time and in continuous time) by an “analog LFSR”, which was obtained by embedding the discrete state space of the LFSR into a larger continuous state space. In this paper, we derived such dynamical systems from message passing algorithms for statistical state estimation. First, we noted that the soft LFSR proposed by Yang and Hanzo may be obtained by forward-only message passing through a factor graph. Second, we proposed a new continuous-time analog of both the LFSR and the soft LFSR that can be realized as a practical electronic circuit. We have thus established a connection between statistical state estimation and the phenomenon of entrainment of dynamical systems. It follows that dynamical systems (e.g., electronic circuits) with better entrainment capabilities may be obtained from more powerful (more complex) message passing algorithms.

9 Acknowledgement

The authors are indebted to Mr. Thomas Schärer of ETH Zurich who built the hardware.

Appendix:

Alternative Message Update Rules for the Soft LFSR

For the convenience of the reader, we explicitly state all computations in the soft LFSR for an alternative (more standard) version of the sum-product algorithm, for the max-product (min-sum) algorithm, as well as for the analog LFSR of Gershenfeld and Grinstein.

A.1 Sum-Product LFSR for Likelihood Ratio Representation

If the messages represent the *ratio* $\tilde{p}(0)/\tilde{p}(1)$ of the pseudo-probabilities, the sum-product update rules of the soft LFSR are as follows.

Initialization: $\mu_k = 1$ for $k = -m + 1, -m + 2, \dots, 0$.

Recursion (for $k = 1, 2, 3, \dots$):

$$\mu_{A,k} = \frac{p(y_k|x_k = 0)}{p(y_k|x_k = 1)} \quad (18)$$

$$\stackrel{\text{for AWGN}}{=} \exp(2y_k/\sigma^2) \quad (19)$$

$$\mu_{B,k} = \frac{1 + \mu_{k-\ell} \cdot \mu_{k-m}}{\mu_{k-\ell} + \mu_{k-m}} \quad (20)$$

$$\mu_k = \mu_{A,k} \cdot \mu_{B,k} \quad (21)$$

At any given time k , an estimate of X_k is obtained as

$$\hat{X}_k \triangleq \begin{cases} 0, & \text{if } \mu_k \geq 1 \\ 1, & \text{if } \mu_k < 1 \end{cases} \quad (22)$$

and $[\hat{X}_k] = (\hat{X}_{k-m+1}, \dots, \hat{X}_{k-1}, \hat{X}_k)$ is an estimate of the state $[X_k]$.

A.2 Max-Product (Max-Sum) Soft LFSR

We state the max-product soft LFSR [15], [16] for the case where the messages represent $\ln(\tilde{p}(0)/\tilde{p}(1))$.

Initialization: $\mu_k = 0$ for $k = -m + 1, -m + 2, \dots, 0$.

Recursion (for $k = 1, 2, 3, \dots$):

$$\mu_{A,k} = \ln \frac{p(y_k|x_k = 0)}{p(y_k|x_k = 1)} \quad (23)$$

$$\stackrel{\text{for AWGN}}{=} 2y_k/\sigma^2 \quad (24)$$

$$|\mu_{B,k}| = \max\{|\mu_{k-\ell}|, |\mu_{k-m}|\} \quad (25)$$

$$\text{sgn}(\mu_{B,k}) = \text{sgn}(\mu_{k-\ell}) \cdot \text{sgn}(\mu_{k-m}) \quad (26)$$

$$\mu_k = \mu_{A,k} + \mu_{B,k} \quad (27)$$

where $\text{sgn}(x)$ denotes the sign of x . Finally, we have

$$\hat{X}_k \triangleq \begin{cases} 0, & \text{if } \mu_k \geq 0 \\ 1, & \text{if } \mu_k < 0 \end{cases} \quad (28)$$

In fact, (24) may be replaced by

$$\mu_{A,k} = y_k, \quad (29)$$

which amounts to multiplying all messages by $\sigma^2/2$ and does not change the estimate (28).

A.3 Analog LFSR by Gershenfeld and Grinstein

In [3], Gershenfeld and Grinstein obtained a discrete-time ‘‘analog’’ LFSR by embedding the discrete dynamics of the LFSR into a continuous state space. They showed that such an analog LFSR entrains to a LFSR sequence even if the latter is modulated by a weak data signal. An extension of this approach to continuous time (using ideal continuous-time delay cells) is also given in [3]. In the setup of this paper, the analog LFSR of [3] can be described as follows.

Initialization: $\mu_k = 0$ for $k = -m + 1, -m + 2, \dots, 0$.

Recursion (for $k = 1, 2, 3, \dots$):

$$\mu_{A,k} = y_k \quad (30)$$

$$\mu_{B,k} = \cos \left[\pi \left(\frac{1 - \mu_{k-\ell}}{2} + \frac{1 - \mu_{k-m}}{2} \right) \right] \quad (31)$$

$$\mu_k = (1 - \epsilon) \mu_{B,k} + \epsilon \mu_{A,k} \quad (32)$$

or, alternatively,

$$\mu_k = \begin{cases} \mu_{B,k} & \text{if } ||\mu_{A,k}| - 1| > \delta \\ (1 - \epsilon) \mu_{B,k} + \epsilon \text{sgn}(\mu_{A,k}) & \text{otherwise} \end{cases} \quad (33)$$

and

$$\hat{X}_k \triangleq \begin{cases} 0, & \text{if } \mu_k \geq 0 \\ 1, & \text{if } \mu_k < 0 \end{cases} \quad (34)$$

In this formulation (and differing from [3]), the ‘‘hard’’ logical values 0 and 1 are represented as +1 and -1, respectively. It should be noted that [3] does not explicitly consider noise at all.

In our simulations, we used (33) with $\delta = \infty$ and optimized ϵ (≈ 0.4 for large SNR).

References

- [1] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. 3. Rockville, Maryland, USA: Computer Science Press, 1985.
- [2] A. F. Molisch, *Wideband Wireless Digital Communications*. Prentice Hall, 2001.
- [3] N. Gershenfeld and G. Grinstein, “Entrainment and communication with dissipative pseudorandom dynamics,” *Physical Review Letters*, vol. 74, pp. 5024–5027, June 1995.
- [4] L.-L. Yang and L. Hanzo, “Iterative soft sequential estimation assisted acquisition of m-sequences,” *Electronics Letters*, vol. 38, pp. 1550–1551, Nov. 2002.
- [5] L.-L. Yang and L. Hanzo, “Acquisition of m-sequences using recursive soft sequential estimation,” *IEEE Trans. Communications*, vol. 52, pp. 199–204, Feb. 2004.
- [6] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Physical Review Letters*, vol. 64, pp. 821–824, Feb. 1990.
- [7] K. M. Cuomo and A. V. Oppenheim, “Circuit implementation of synchronized chaos with applications to communications,” *Physical Review Letters*, vol. 71, July 1993.
- [8] A. Abel and W. Schwarz, “Chaos communications—principles, schemes, and system analysis,” *Proc. IEEE*, vol. 90, pp. 691–710, May 2002.
- [9] J. Dauwels, H.-A. Loeliger, P. Merkli, and M. Ostojic, “On structured-summary propagation, LFSR synchronization, and low-complexity trellis decoding,” *Proc. 41st Allerton Conf. on Communication, Control, and Computing*, (Allerton House, Monticello, Illinois), Oct. 1–3, 2003, pp. 459–467.
- [10] J. Dauwels, H.-A. Loeliger, P. Merkli, and M. Ostojic, “On Markov structured summary propagation and LFSR synchronization,” *Proc. 42nd Allerton Conf. on Communication, Control, and Computing*, (Allerton House, Monticello, Illinois), Sept. 29–Oct. 1, 2004, pp. 451–460.
- [11] D. Megnet, H. Mathis, P. Flammant, and A. Thiel, “C/A-code synchronization using analog feedback shift registers (AFSR),” *Proc. ION GNSS 2004*, Long Beach, CA, September 21–24, 2004, pp. 32–42.
- [12] K. M. Chugg and M. Zhu, “A new approach to rapid PN code acquisition using iterative message passing techniques,” *IEEE J. on Selected Areas in Communications*, vol. 23, pp. 884–897, May 2005.
- [13] O. W. Yeung and K. M. Chugg, “An iterative algorithm and low complexity hardware architecture for fast acquisition of long PN codes in UWB systems,” to appear ???.

- [14] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Information Theory*, vol. 20, pp. 284–287, March 1974.
- [15] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Information Theory*, vol. 47, pp. 498–519, Feb. 2001.
- [16] H.-A. Loeliger, "An introduction to factor graphs," *IEEE Signal Proc. Mag.*, Jan. 2004, pp. 28–41.
- [17] T. Koch, *Continuous-Time Synchronization*. Semester Project, Signal and Information Processing Laboratory, ETH Zurich, Switzerland, July 2003.
- [18] H.-A. Loeliger, F. Lustenberger, M. Helfenstein, and F. Tarköy, "Probability propagation and decoding in analog VLSI," *IEEE Trans. Information Theory*, vol. 47, pp. 837–843, Feb. 2001.
- [19] F. Lustenberger *On the Design of Analog VLSI Iterative Decoders*. PhD thesis at ETH Zurich, Diss. ETH No 13879, Nov. 2000.
- [20] H.-A. Loeliger, "Analog decoding and beyond," *Proc. 2001 IEEE Information Theory Workshop*, Cairns, Australia, Sept. 2–7, 2001, pp. 126–127.
- [21] P. Merkli, *Message-Passing Algorithms and Analog Electronic Circuits*. PhD thesis at ETH Zurich, Diss. ETH No 15942, April 2005.