GENERATION OF GOLD-SEQUENCES WITH APPLICATIONS TO SPREAD SPECTRUM SYSTEMS

F. Rodríguez Henríquez (1), *Member, IEEE,* N. Cruz Cortés (1), *Member, IEEE,* J.M. Rocha-Pérez (2)
Member, IEEE. F. Amaro Sánchez (3).

***Abstract*--In this paper we discuss some of the most relevant theoretical and practical aspects related to the Hardware implementation of pseudo-random Gold-sequences. The main contribution of this work is the proposal of a general methodology that allows us to generate Gold-sequences for any arbitrary order in an efficient way. A specific design example that illustrates how to use our method to obtain a set of Gold-sequences of order n=5 together with its application in a simplified spread spectrum communications system is also given. All the results presented here were tested and simulated via MatLab programs that were written following our proposed methodology.**

***Index terms*— Gold sequences, Pseudo-random sequences, Spread spectrum.**

I. INTRODUCTION

The ever increasing importance of application areas such as cryptography and spread-spectrum communications has led to a renovated interest in periodic correlation parameters for pseudorandom sequences. Spread spectrum modulation uses a transmission bandwidth many times greater than the information bandwidth. For this kind of systems, the first issue that a designer needs to solve is the generation of a noise-like signal. Similarly, most cryptographic areas need the implementation of pseudo-random periodic sequences with high cross-correlation properties.

The study of pseudorandom and related sequences spans for more than fifty years. During that time, results have been obtained on structural properties, correlation functions, method of generation, and applications to various electronic systems problems.

So far, the sequences that have received more attention in the literature are the maximal-length linear feedback shift register binary sequences, which we refer to as m-sequences. As the name suggests, these are precisely the sequences of maximum possible period (which is $N = 2^n - 1$) that can be obtained from an n-stage binary shift register with linear feedback.

One of the key features of an m-sequence is its autocorrelation function $\theta_{x,x}(0) = N$ and $\theta_{x,x}(l) = -1$ for $1 \le l < N$. It is this ideal periodic autocorrelation property that was exploited in most of the early applications of the m-sequences.

The mathematical study of maximal-length sequences (m-sequences) seems to have started in the mid-1950s. Much of the early research was concerned with the autocorrelation properties and the “noise-like” aspects of m-sequences. However, some attention was given to the problem of selecting sets of m-sequences with good cross-correlation properties and by the late 1960’s several theoretical and experimental results were known. However, even at the present time the key cross-correlation properties of m-sequences are considerably less widely known than the autocorrelation properties, and yet the former is more important in many applications such as the ones mentioned above.

The main design problem address in this paper is how to generate in the cheapest way, Gaussian noise signals with low cross-correlation values. There are two quite important characteristics that this generation technique should exhibit:

- Implementation. Should be easily implemented and reproducible; because the same generating process must be used at the transmitter (for encoding/spreading); and at the receiver (for decoding/undo-spreading).
- The signals generated at the receiver must be perfectly synchronized with the timing of the received transmission.

In this research work we describe a practical methodology to generate a special class of periodic m-sequences called Gold sequences. Gold sequences yield the theoretically minimum cross-correlation values that one can possibly expect from periodic m-sequences. Implementation details and the application of Gold sequences to spread spectrum systems are also outlined.

The remaining part of this paper is organized as follows. Section II introduces the most important mathematical concepts and definitions related to m-sequences in general and their related cross-correlation properties. Also in section II a three-step strategy that allows us to generate Gold

1. CINVESTAV-IPN, Computer Science Section.
Av. IPN 2508, 07360 México, D.F.
2. INAOE, Tonantzintla, Puebla.
3. BUAP, Facultad de Electrónica

sequences in a practical manner is outlined. That strategy was coded in MatLab and in section III the corresponding implementation details are fully discussed. Then, in section IV we present a design example of a spread spectrum system using a Gold sequence of order five. Final conclusions and remarks are given in section V.

II. Mathematical Background

We start our discussion with the following mathematical definitions. Let $h(x) = h_0 x^n + h_1 x^{n-1} + ... + h_{n-1} x + h_n$ denote a binary monic polynomial of degree n where $h_0 = h_n = 1$ and the other h_i's can take values of 0 or 1. It is customary to represent such polynomial as a binary vector $h = (h_0, h_1, ..., h_n)$, and to express that vector in octal notation. For example, the polynomials $x^4 + x + 1$ and $x^5 + x^2 + 1$ are represented by the binary vectors 10011 and 100101, respectively, and the octal notation for those polynomials is 23 and 45, respectively.

A periodic binary sequence u is said to be a sequence generated by the binary polynomial $h(x)$ defined above if for all integers j:

$$h_0 u_j \oplus h_1 u_{j-1} \oplus h_2 u_{j-2} \oplus ... \oplus h_n u_{j-n} = 0 \qquad (1)$$

A given polynomial $h(x)$ is called primitive, if its associated periodic sequence has the maximum theoretical period of repetition given by $N = 2^n$-1.

From equation (1) it follows that the periodic sequence u can be generated by an n-stage binary linear feedback shift register which has a feedback tap connected to the i-th cell if $h_i = 1$, $0 < i <$ n as is shown in Fig. 1 [Glissic95, Viterbi95]. Notice that since $h_n = 1$, there is always a connection for the nth cell.

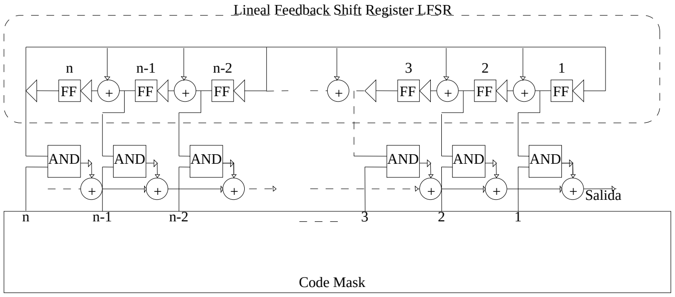

Fig. 1 Realization of a maximum length sequence

A shift register can generate several different periodic sequences, one of which is the all-zeroes sequence. Of course, only the nonzero sequences are of interest. The following properties of shift register periodic sequences are well known and are stated here for convenience:

- If $\boldsymbol{u}$ is a periodic sequence generated by $h(x)$, then for all integers i, $T^i\boldsymbol{u}$ is also a sequence generated by $h(x)$; where the operator T^i shifts the periodic sequence u by i places. Hence, any shift register can generate different phases of the same periodic sequence.
- If $\boldsymbol{u}$ and $\boldsymbol{v}$ are generated by $h(x)$, then so is $\boldsymbol{u} \oplus \boldsymbol{v}$.
- The period of $\boldsymbol{u}$ is at most $N = 2^n$-1, where n is the number of cells in the shift register, or equivalently, the degree of $h(x)$.
- There are exactly N nonzero periodic sequences generated by $h(x)$, and they are just N different phases of $\boldsymbol{u}$; namely $\boldsymbol{u}$, T$\boldsymbol{u}$, T$^2\boldsymbol{u}$, …, T$^{N-1}\boldsymbol{u}$.
- A sequence of period N is a maximum length sequence if and only if it has the *shift-and-add* property, which can be formulated as follows. Given distinct integers i and j, $0 \leq i, j <$ N, there is a unique integer k, distinct from i and j, such that $0 \leq k <$ N and: $T^i u \oplus T^j u = T^k u$.

In most practical applications, a binary sequence is actually transmitted as a sequence of positive and negative pulses of unit amplitude. By convention, the waveform to be transmitted is obtained by replacing each 1 of the original binary sequence by a –1 and each 0 by a +1. We can map any arbitrary {0, 1}-valued periodic sequence $\boldsymbol{u}$, by using the function χ such that:

$$\chi(\alpha) = (-1)^{\alpha} \text{ for } \alpha \in \{0, 1\}. \qquad (2)$$

Notice that $T^i(\chi(u)) = \chi(T^i u)$ and

$$\sum \chi(u) = \chi(u_0) + \chi(u_1) + ... + \chi(u_{N-1}) = N - 2hw(u) \qquad (3)$$

Where $hw(\boldsymbol{u})$ denotes the Hamming weight of $\boldsymbol{u}$, and N is the period of the sequence u.

Having defined binary periodic sequences and their associated generating polynomial, let us define now the important concept of periodic cross-correlation between sequences.

Definition 1 For sequences x and y of period N, we define the periodic cross-correlation function by:

$$\theta_{x,y}(l) = \sum_{n=0}^{N-1} x_n y_{n+l} \qquad (4)$$

It is straightforward to verify that for each $l \in$Z,

$$\theta_{x,y}(l) = \theta_{x,y}(l + N) \qquad (5)$$

Also, we define the periodic auto-correlation function $\theta_x(l)$ for the sequence x as $\theta_{x,x}(l)$.

Within the context of applications for spread-spectrum communications we are interested in the problem of how to find sets of periodic pseudo-random sequences with the following two properties:

- For each sequence $x = x_n$ in the set, $|\theta_{x,x}(l)|$ is as small as possible for $1 \leq l \leq$ N-1;
- For each pair of sequences $x = x_n$ and $y = y_n$, $|\theta_{x,y}(l)|$ is as small as possible for all l.

Sequences that exhibit the above two properties and the design problem of how to implement them efficiently in hardware are the main subject of this paper. In the remaining part of this section, we will derive the theoretically best results that one can possibly expect from such a set of periodic sequences.

Applying the definition given in (2) to the cross-correlation formula of equation (4) we obtain:

$$\begin{aligned}\theta_{u,v}(l) \overset{\Delta}{=} \theta_{\chi(u),\chi(v)}(l) &= \sum_{i=0}^{N-1}\chi(u_i)\chi(v_{i+l}) \\ &= \sum_{i=0}^{N-1}(-1)^{u_i}(-1)^{v_{i+l}} \\ &= \sum_{i=0}^{N-1}(-1)^{u_i \oplus v_{i+l}} \\ &= \sum_{i=0}^{N-1}\chi(u_i \oplus v_{i+l})\end{aligned} \tag{6}$$

Plugging the result of equation (3) into the last equation, we obtain:

$$\theta_{u,v}(l) = N - 2hw(u \oplus T^l v) \tag{7}$$

Let us now, define $t(n)$ as

$$t(n) = 1 + 2^{\left\lfloor \frac{n+2}{2} \right\rfloor}, \tag{8}$$

Where $\lfloor \alpha \rfloor$ denotes the integer part of the real number α. Then with $n \neq 0 \bmod 4$, there always exist pairs of sequences with three valued cross-correlation functions, where the three values are: -1, $-t(n)$, and $t(n)$–2 [Prasad96, Ziemer92, Simon94]. A cross-correlation function taking these and only these values is called preferred three-valued cross-correlation function and the corresponding pair of polynomials associated with it, is called a *preferred pair of polynomials*.

In the next subsection we will show how to use a *preferred pair of polynomials* to generate a set of pseudo-random sequences with theoretical-minimum cross-correlation values.

A. Gold Sequences

Gold sequences form an important class of periodic sequences, which provide larger sets of sequences with good periodic cross-correlation. A set of Gold sequences of period $N = 2^n - 1$, consists of N+2 sequences for which we have excellent cross-correlation properties. A set of Gold sequences can be constructed from appropriately selected maximum length sequences as described below.

Suppose a shift register polynomial $f(x)$ factors into $h(x)g(x)$ where $h(x)$ and $g(x)$ have no factors in common. Then the set of all sequences generated by $f(x)$ is just the 8set of all sequences of the form $a \oplus b$ where a is some sequence generated by $h(x)$, b is some sequence generated by $g(x)$, and where both, a and b can be either nonzero or zero sequences.

Assuming now that $h(x)$ and $g(x)$ are two preferred pair of primitive polynomials of degree n and that each one of them generates the m-sequences $\boldsymbol{u}$ and $\boldsymbol{v}$ of maximum period $N = 2^n$-1, respectively. If y denotes a nonzero sequence generated by $f(x) = h(x)g(x)$ then, from the above properties of m-sequences, we get that either:

$$\begin{aligned} & y = T^i u; \\ or\quad & y = T^j v; \\ or\quad & y = T^i u \oplus T^j v. \end{aligned} \tag{9}$$

Where $0 \leq i, j \leq N$-1. From equation (9) it follows that y must be some phase of one of the sequences in the set G($\boldsymbol{u}$, $\boldsymbol{v}$) defined as,

$$G(u,v) \equiv \{u, v, u \oplus v, u \oplus Tv, u \oplus T^2 v, \ldots, u \oplus T^{N-1} v\} \tag{10}$$

Note that G($\boldsymbol{u}$, $\boldsymbol{v}$) contains a total of N =2 = 2^n + 1 sequences of period N. Every single pair of sequences that belongs to the set G($\boldsymbol{u}$, $\boldsymbol{v}$), has the property that its cross-correlation function can only take one of the three different values defined for the preferred pair of sequences: -1, -t(n), and t(n)–2.

Therefore, in order to construct a Gold-sequence set for a given order n, we can use the following methodology:

1) Find a preferred pair of primitive polynomials $h(x)$ and $g(x)$ of order n.

2) By using the shift-register architecture, implement the sequences u and v corresponding to the polynomials $h(x)$ and $g(x)$, respectively.

3) Use the N different phases of either $\boldsymbol{u}$ or $\boldsymbol{v}$, in order to find each of the N+2 Gold sequences as they are given in equation (10).

In the next section we explain how we can obtain Gold sequences based on the above three-step strategy.

```
Input:   Two monic polynomials of degree n P1, P2
Output:  Cross-correlation plot.
function o    = crossc(poly1, poly2)
% 0 Initialization
         figure(2); crossc = [];
% 1. Generating sequences u, v from the gen. polynomials.
         u          = pn(poly1);
         v          = pn(poly2);
% 2. Finding the order&length of the generator polynomials.
         ord        = length(oct2bin(poly1));
         N          = (2^(ord-1) - 1)*2;
% 3. Obtaining the periodic Cross-correlation spectrum
% if poly1 and poly2 form a preferred pair of m sequences
% then, its cross-correlation can only take three values: 1, -%
t(n) and t(n) - 2, where t(n) = 1+ 2^|(n+2)/2|
         for        i    = 0: N-1
% 4 Crosscorralating with shift i.
         crossc = [crossc sum(summ(u, [v(1+i: N) v(1:i)]))];
         end
% 5 Plotting.
         Figure; stem(crossc);
         grid; title('Crosscorrelation function');
         xlabel('Shift (from 0 to N-1)'); ylabel('Teta');
```

Figure 2. Finding the cross-correlation of two primitive polynomials.

III. GENERATION OF GOLD SEQUENCES

According to the methodology outlined in the last section, the first problem that a designer needs to face in order to generate a set of gold sequences is to find eligible couples of polynomials (i.e. couples of primitive polynomials) candidates to conform a *preferred pair of polynomials*. The problem to calculate all possible primitive polynomials is unfeasible because their grown is exponential with the order *n*. For example, for *n=20*, the number of primitive polynomial is 24,000. Fortunately there are several heuristic and probabilistic tests that efficiently determine if a given polynomial is primitive or not. In the rest of this section we will assume that the user possesses a list of primitive polynomials of the desired order *n*.

In order to test if two primitive polynomials have or not the preferred cross-correlation characteristic, we can use the MatLab-like pseudo-code shown in Fig. 2.

For *n* = 7, the algorithm in Fig. 2 finds (among others) the following candidates as a *preferred pair of polynomials* (all of them in octal representation): 221 and 345; 211and 217; 211 and 247; 211 and 235; 301and 313, etc. On the other hand, one can check that the pair of primitive polynomials: 211 and 221; 313 and 323, do not form a preferred pair of polynomials. Those results completely agree with the diagram of maximum connected sets described in [Sarwate80].

Fig. 3 shows a code that stores all the Gold-sequences generated by a preferred pair of polynomials. The output matrix has a size of *N*+2 rows and *N*-1 columns, and it contains all the *N*+2 gold sequences associated with the preferred pair, each of them having a total length of *N*-1 (where $N = 2^n\text{-}1$, and where n is the given order of the primitive polynomials).

Input: Two preferred monic polys of degree n P1, P2
Output: Associated Gold Sequences

```
function seq_m       = gold(poly1, poly2)
% Each row of the seq_m matrix, contains one of the 2^n +1
% Gold sequences generated by the given preferred pair of
  % polynomials poly1 and poly2.
% 0 Initialization
          figure;
% 1. Generating sequences u, v from the gen. polynomials.
          u          = pn(poly1);
          v          = pn(poly2);
% 2. Finding the order&length of the generator polynomials.
          ord        = length(oct2bin(poly1));
          N          = (2^(ord-1) - 1)*2;
% 3. Generation of Gold Sequences.
          seq_m(1,:) = u;
          seq_m(2,:) = v;
          for i = 1: N
                  seq_m(i+2,:) = u.*[v(1+i: N) v(1:i)];
          end
```

Fig. 3 Generation of a Gold Sequence set.

IV. IMPLEMENTATION EXAMPLE

In this section we present an explicit example of how the generation of a set of Gold sequences of order n=5 can be used in practice on a spread spectrum communications system.

Let us discuss first the simplified spread spectrum system shown in Figure 4, where it is assumed that all the users subscribed to the system may gain simultaneous access to the channel in a Code-Division Multiple Access (CDMA) fashion.

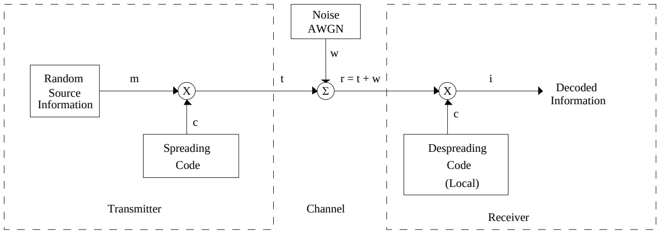

Fig. 4 Spread Spectrum concept

In the transmitter side of the system shown in Fig. 4, a random binary message *m*, with bandwidth *B* is spread into a bandwidth *PG* times greater through the use of a pseudorandom *PN* sequence *c*. *PG* is called the processing gain. We also assume that the distortion introduced by the channel can be modeled as an additive white Gaussian noise, *AWGN* composed of two main components: The white noise intrinsic to the channel and, the noise contribution of all the other users sharing the channel.

In the receiver side, a process of de-spreading is carried out by multiplying the received signal with an exact copy of the *PN* sequence used during transmission. The received signal (before de-spreading) looks as shown in Figure 5. However, after the process of de-spreading is performed, the system is able to recover the original information, as is shown in Fig. 6, where both, the original and the recovered signals can be compared.

It is apparent that for this kind of systems the generation of high quality pseudorandom m-sequences is one of the crucial design issues in order to obtain a correct performance of the communications system.

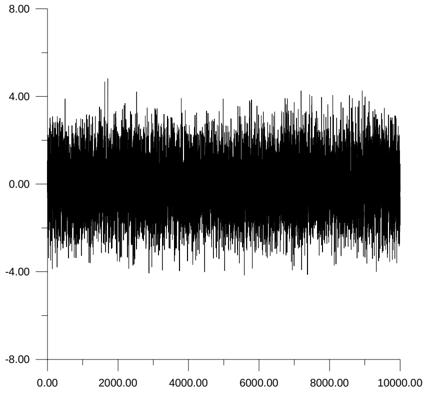

Fig. 5 Typical received signal (information + noise).

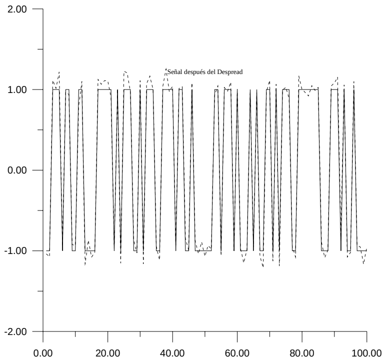

Fig. 6 Comparison between the original (continuous line) and the recovered (dashed line) information

As it was explained in section II, Gold sequences are a special class of m-sequences that happen to be particularly suitable for spread spectrum applications. An attractive characteristic of this kind of sequences is that the generated sequences are very easy and cheap to implement, and hence, they represent a good option when compared with other realizations. Also in section II, it was pointed out that it is always possible to obtain special pairs of Gold m-sequences having a three-valued cross-correlation function among them [Prasad96, Ziemer92, and Simon94]. For example, for *n=10*, using equation (8), we have $t(10) = 2^6+1=65$ and the only three values for the cross-correlation function of the preferred Gold sequences will be: {-1, -65, 63}.

For spread spectrum applications, we can choose the length of the sequence according to the desired capacity of the channel (in terms of the number of users). Since the spread spectrum processing gain PG is directly proportional to the length of the m-sequences, a more common criterion used frequently in practice is to select first the gain (in dB) in order to comply with some given specification in the reception side of the communication channel [Jen-Shi97].

Once that the length of the sequences has been fixed we need to select a pair of preferred sequences. A different initial phase of the sequence can be assigned to each user in the system. In this way, each user has a code that identifies him/her uniquely.

As an illustrative example, let *n=5* be the required order for a set of Gold sequences. In order to find a preferred pair of m-sequences we fed the primitives polynomials in octal notation to the Matlab program shown in Fig. 2. The program gives information about which polynomials form preferred pairs. For the case in hand, the program found the pair 45 and 75 as one of the preferred pairs. With this information we can construct the circuit of Figure 7.

It is very important to verify that the circuit indeed accomplishes the cross-correlation property defined by equation (8). The plot of the corresponding cross-correlation function is obtained with the Matlab code of Fig. 2. Notice that for this case *n=5*, hence *t(n) = {-1, -9, 7}*. As we can see in Fig. 8, the cross-correlation function values obtained correspond to the predicted ones.

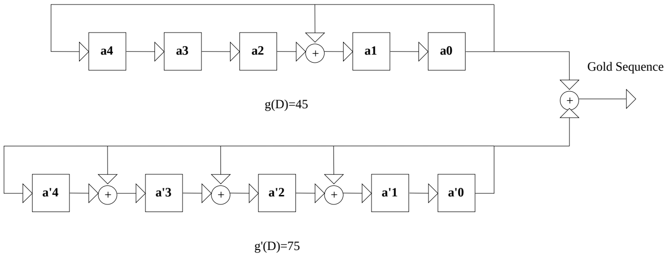

Fig. 7 Gold sequence generator

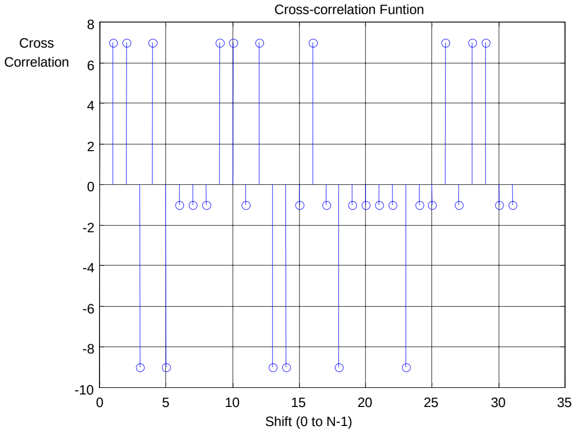

Fig. 8 Cross-correlation function for Gold sequences of order 5.

V. CONCLUSIONS

The most important properties of m-sequences, Gold sequences and their application to spread spectrum have been presented. Gold-sequence implementation requires finding a preferred pair of m-sequences which is in general a difficult task. In this paper an efficient and practical methodology has been introduced together with its corresponding Matlab implementation. By following our methodology and through the use of our Matlab-coded algorithms we can find and generate preferred m-sequences and therefore we can construct Gold sequences of any order. For illustration purposes a specific design example for Golden sequences of order n=5 was presented, although the program is able to find preferred pairs of any order.

V. REFERENCES

[Flikkema97] Flikkema, Paul G., *Spread Spectrum Techniques for Wireless Communication* IEEE Signal Processing Magazine, May 1997.

[Ziemer92] Ziemer Rodger E., Peterson Roger L., *Introduction to Digital Communication*, MacMillan Publishing Company, 1992.

[Glisic95] Glisic Savo G., Leppanen Pentti A., *Code Division Multiple Access*, Kluwer Academic Publishers, 1995

[Pickholtz82] Pickholtz, Schilling, Laurence, Milstein, *Theory of Spread Spectrum Communications* - A Tutorial, IEEE Trans. on Comm, May 1982.

[Viterbi95] Viterbi Andrew J., *CDMA Principles of Spread Spectrum Communication*, Addison-Wesley Publishing Company, 1995

[Jen-Shi97] Jen-Shi Wu, et al, *A 2.6-V, 44-Mhz All-Digitall OPSK Direct-Sequence Spread-Spectrum Transceiver IC*, IEEE JSSC, October 1997.
[Prasad96] Prasad Ramjee, *CDMA for Wireless Communications*, Artech House, 1996.
[Simon94] Simon, Marvin K. Et al, *Spread Spectrum Communications Handbook*, Mc Graw-Hill, 1994.