Toward an Approximation Theory for Computerised Control*

Paul Caspi[1], Albert Benveniste[2]

[1] Verimag (CNRS), Centre Equation, 2, rue de Vignate, 38610 Gieres, France
caspi@imag.fr
http://www-verimag.imag.fr/VERIMAG/
[2] Irisa/Inria, Campus de Beaulieu, F-35042 Rennes cedex, France
benveniste@irisa.fr
http://www.irisa.fr/sigma2/

Abstract. This paper addresses the question of extending the usual approximation and sampling theory of continuous signals and systems to those encompassing discontinuities, such as found in modern complex control systems (mode switches for instance). We provide some evidence that the Skorokhod topology is a good candidate for dealing with those cases in a uniform manner by showing that, in the boolean case, Skorokhod uniformly continuous signals are exactly the signals with uniform bounded variability.

1 Introduction

1.1 Problem statement

The question of how accurately a control system can be implemented on computers is clearly an important one. For instance, this question arises when a satisfactory control system has been obtained and has to be implemented: how the uncertainties arising from a computer implementation will impair the obtained results in terms of *e.g.*, stability? This question also arises when considering fault tolerance: in highly critical systems, fault tolerance is achieved by massive redundancy and voting. Though the computer science view of fault tolerance advocates the use of exact voting (two redundant units should agree bit-wise on their results)[11,8], in many systems, for instance in the Airbus "fly-by-wire" systems, a smoother approach is taken which can be seen as a "topological" approach. It consists of determining a "normal operation" neighbourhood into which signals should stay according to the several sources of uncertainty that can impair them. Then, the idea is that faults are detected if signals do not belong to the same neighbourhood [5].

This question is a classical one, as far as "continuous control" is considered and can be addressed by using classical distances. But modern control systems are more and more based on mixed (or "hybrid") techniques encompassing also non continuous computations: switches, modes, etc.

* This work has been partially supported by Esprit R&D project CRISYS EP 25514 and by Airbus-Verimag contracts 2001-2002

Our paper tries to extend the "classical approach" to these "hybrid systems". In a first section, we present this classical approach. We show here how approximation and sampling can be dealt with in terms of uniform continuity. In a second section, we consider the case of discontinuous signals and systems. Uniform bounded variability seems to appear here as the analogue of uniform continuity, in that it characterises "slow" varying signals that can be thoroughly sampled without loosing too much information. However, uniform bounded variability doesn't provide a nice topological framework. In the third section, we show that the Skorokhod distance gives us the missing topological framework as we can show that uniform bounded variability signals are exactly those which are Skorokhod uniformly continuous. Furthermore, it encompasses both cases, continuous and non continuous, and thus allows to deal with hybrid cases.

1.2 Related Works

Several approaches seem to have been followed for addressing the question:

- The topological approach initiated by Nerode [12,3] explicitly introduces the approximation and then tries to characterise it as a continuous mapping. This leads to equip the approximation space with an *ad-hoc* (small) topology.
- The equivalence or property preserving approaches followed for instance in [10,1,6,7] tries to construct an approximation of a given system and to check whether it is equivalent to or preserves some properties of the original system expressed in some logic.
- Finally, M. Broucke [9] mixes the two approaches and uses the Skorokhod distance in order to define an approximate bisimulation between several classes of hybrid systems. In this sense, her work is quite close from ours. However, the motivations are slightly different: it doesn't seem that uniformity is addressed and that a result similar to theorem 4 is obtained.

2 The Classical Continuous Framework

2.1 Basic Definitions

We consider systems that have to operate continuously for a long time for instance a nuclear plant control that is in operations for weeks or an aircraft control that flies for several hours. Thus, the horizon of our signals is not bounded. Hence, a *signal* x is for us simply a function from R^+ to R and a *system* is simply a function f causally transforming signals, that is to say, such that $f(x)(t)$ is only function of $x(t'), t' \leq t$.

The *delay operator* Δ^τ is such that $(\Delta^\tau x)(t) = x(t-\tau)$, and a system is *stationary* (or time invariant) if $\forall \tau, S(\Delta^\tau x) = \Delta^\tau(S x)$.

A signal x is *uniformly continuous (UC)* (figure 1) if there exists a positive function η_x from errors to delays, such that:

$$\forall \varepsilon > 0, \forall t, t', |t-t'| \leq \eta_x(\varepsilon) \Rightarrow |x(t) - x(t')| \leq \varepsilon$$

Such a definition can be rephrased in a functional way by introducing the $||\ ||_\infty$ norm on signals, defined as

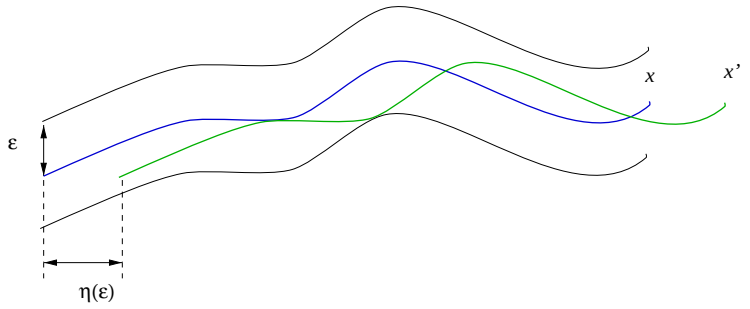

Fig. 1. A uniformly continuous signal

$$||x||_\infty = \inf_{x' \approx x} \sup_{t \in R^+} |x'(t)|$$

where $\approx$ denotes the equality "almost every where", that is to say such that isolated discontinuity points are not taken into account.

Then, a signal x is uniformly continuous if there exists a positive function η_x from errors to delays, such that:

$$\forall \varepsilon > 0, \forall \tau, |\tau| \leq \eta_x(\varepsilon) \Rightarrow ||x - \Delta^\tau x)||_\infty \leq \varepsilon$$

2.2 Retiming and Sampling

A *retiming* function is a non decreasing function from R^+ to R^+. This is a very general definition which has many possibilities. For instance, a piece-wise constant retiming function can be seen as a sampler: if $x' = x \circ r$, and if r is piece-wise constant, then, at each jump of r, a new value of x is taken and maintained up to the next jump. This allows us to define a periodic sampler r, of period T_r by the piece-wise constant function:

$$r(t) = E(t/T_r)$$

where E is the integer part function (see figure refpersamp).

Retiming allows us to restate the uniformly continuous signal definition, by saying that a signal x is uniformly continuous if there exists a positive function η_x from errors to delays, such that:

$$\forall \varepsilon > 0, \forall \, retiming \, r, ||r - id||_\infty \leq \eta_x(\varepsilon) \Rightarrow ||x - x \circ r||_\infty \leq \varepsilon$$

where *id* is the identity retiming function.

We can then define a *samplable* signal as a signal such that the sampling error can be controlled by tuning the sampling period:

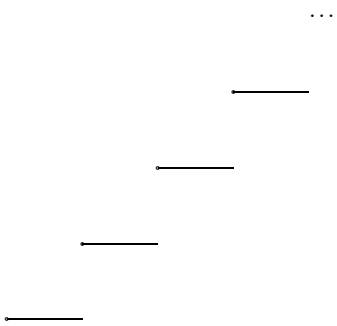

Fig. 2. A periodic sampling retiming

Definition 1 (Samplable Signal). *A signal x is samplable if there exists a positive function η_x from errors to sampling periods, such that:*

$$\forall \varepsilon > 0, \forall \text{ periodic sampling } r, T_r \leq \eta_x(\varepsilon) \Rightarrow ||x - x \circ r||_\infty \leq \varepsilon$$

Then the following theorem obviously holds:

Theorem 1. *A signal is samplable if and only if it is uniformly continuous.*

2.3 From Signals to Systems

This framework extends quite straightforwardly to systems by saying that a system S is uniformly continuous (figure 3) if there exists a positive function η_S from errors to errors such that:

$$\forall \varepsilon > 0, \forall x, x', ||x - x'||_\infty \leq \eta_S(\varepsilon) \Rightarrow ||(S\,x) - (S\,x')||_\infty \leq \varepsilon$$

and state the following theorem:

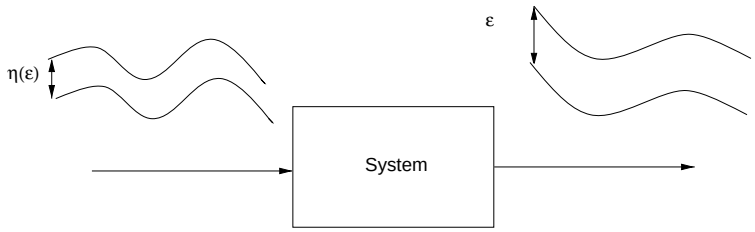

Fig. 3. A uniformly continuous system

Theorem 2. *A uniformly continuous stationary system, fed with a uniformly continuous signal outputs a uniformly continuous signal.*

Proof. Given x UC, S UC, and $\varepsilon > 0$,

$$\forall x', ||x - x'||_\infty \leq \eta_S(\varepsilon) \Rightarrow ||(S\,x) - (S\,x')||_\infty \leq \varepsilon$$

and

$$\forall \tau, |\tau| \leq \eta_x(\eta_S(\varepsilon)) \Rightarrow ||x - (\Delta^\tau\, x)||_\infty \leq \eta_S(\varepsilon)$$

Thus,

$$\forall \tau, |\tau| \leq \eta_x(\eta_S(\varepsilon)) \Rightarrow ||(S\,x) - (S\,(\Delta^\tau\, x)||_\infty \leq \varepsilon$$

But $S(\Delta^\tau\, x) = \Delta^\tau(S\,x)$. We thus get

$$\eta_{Sx} = \eta_x \circ \eta_S$$

This theorem says that given an acyclic network of UC systems, one can compute maximum delays on system interconnection, sampling periods and maximum errors on input signals such that errors on output signals be lower than given bounds. This provides us thus with a nice approximation theory.

2.4 Generalisation

This extends to any distance between signals:

Definition 2 (Uniformly continuous signals). *A signal x is UC for the distance d if there exists a positive, error to delay function η_x such that:*

$$\forall \varepsilon > 0, \forall \tau, |\tau| \leq \eta_x(\varepsilon) \Rightarrow d(x, \Delta^\tau\, x) \leq \varepsilon$$

Definition 3 (Uniformly continuous systems). *A system is UC for the distance d if there exists a positive, error to error function η_S such that:*

$$\forall \varepsilon > 0, \forall x, x', d(x, x') \leq \eta_S(\varepsilon) \Rightarrow d((S\,x), (S\,x')) \leq \varepsilon$$

In this generalised background, the same theorem holds:

Theorem 3. *A uniformly continuous stationary system S, fed with a uniformly continuous signal x outputs a uniformly continuous signal:*

$$\eta_{Sx} = \eta_x \circ \eta_S$$

3 Uniform Bounded Variability Signals

We now consider boolean signals and we want to find some concept more or less equivalent to uniform continuity in the sense that it characterises "slowly" varying signals that can be sampled. For the sake of simplicity, we restrict ourselves in the remaining of the paper to *piece-wise continuous* signals, *i.e.*, signals for which there exists an increasing and either finite or diverging sequence of times $\{t_0, \ldots t_n, \ldots\}$ such that the signal is continuous in every open interval $]t_n, t_{n+1}[$. For this kind of signal we can introduce a *discontinuity count function*

Definition 4 (Discontinuity count function). *$dc_{t_1,t_2}(x)$ is the function counting the number of discontinuity points of a signal x in an interval $[t_1, t_2]$.*

$$dc_{t_1,t_2}(x) = card\{t \mid x(t^-) \neq x(t^+) \wedge t_1 \leq t \leq t_2\}$$

where, as usual, $x(t^-), (x(t^+))$ is the left (right) limit of x at t.

When applied to boolean signals, this allows us to define these "slowly varying signals" as those signals which only have a bounded number of discontinuities in any time interval of given length:

Definition 5 (Uniform bounded variability signal (UBV)). *A boolean signal x has UBV (figure 4) if there exists a function from discontinuity counts to delays, η_x, such that:*

$$\forall n \in N^+, \forall t, t', |t - t'| \leq \eta_x(n) \Rightarrow dc_{t,t'}(x) \leq n$$

where N^+ denotes the set of positive integers. This definition "patches" the continuity one, but, in general the only interesting value for n is 1. Then $T_x = \eta_x(1)$ is the minimum stable time of the signal.

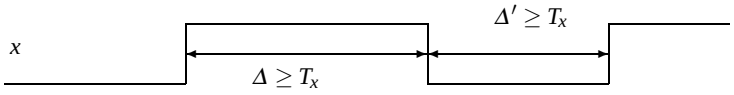

Fig. 4. Uniform bounded variability

This definition could allow us to adapt the previous approximation theory to boolean signals. For instance we could define *samplable* boolean signal, as those signals for which a sampling period can be found such that a given minimum number of samples can be drawn at each constant valued interval. Then, clearly, samplable boolean signals correspond to uniform bounded variability ones.

However, this is not a topological definition and it lacks many of its appealing features, e.g., triangular inequality. For instance we cannot derive from it a convenient definition for systems. Furthermore, it is not clear how this definition combines with the classical one for mixed signals.

4 Skorokhod Distance

4.1 Definition

This distance [2] has been proposed as a generalisation of the usual distance so as to account for discontinuities.

Definition 6 (Skorokhod distance).

$$d_S(x,y) = \inf_{bijective\ retiming\ r} ||r-id||_\infty + ||x-y\circ r||_\infty$$

We see here the idea of this definition: instead of comparing the signals at the same times, we allow shifts in time before comparing points, provided the shifts are bijective, i.e., we don't miss any time. In this definition, the use of bijective retimings is fundamental. Otherwise, it could be easily shown that it would not be a distance: for instance symmetry and triangular inequality could be violated.

4.2 Skorokhod Distance and Uniform Bounded Variability

Let us show here that the Skorokhod distance can replace the non topological concept of uniform bounded variability. This is the main result of the paper and is summarised in the following theorem:

Theorem 4. *A boolean signal has uniform bounded variability if and only if it is Skorokhod uniformly continuous.*

Proof. The proof is based on the following lemmas:

Lemma 1. *A bijective retiming is both increasing and continuous and its inverse is continuous: it is an homeomorphism.*

This is a classical property whose proof is omitted.

Lemma 2. *If r is a bijective retiming with $||r-id||_\infty \leq \delta$, then*

$$dc_{0,t-\delta}(x) \leq dc_{0,t}(x\circ r) \leq dc_{0,t+\delta}(x)$$

In other words, a bounded bijective retiming preserves the number of discontinuities. This is due to the fact that is is an homeomorphism which preserves limits.

The proof then proceeds as follows:

Only if part: Let T_x be the minimum stable time associated with x. Let us show that x has $\eta_x(\varepsilon) = \inf\{\varepsilon, \frac{T_x}{3}\}$ as time to error function.

Let r be a retiming with $||r-id||_\infty \leq \eta_x(\varepsilon)$ and t a discontinuity point of x with, for instance $x(t^-) = 0, x(t^+) = 1$. We then have:

$$t' \in [t - \frac{T_x}{2}, t[\Rightarrow x(t') = 0$$
$$t' \in]t, t + \frac{T_x}{2}] \Rightarrow x(t') = 1$$

r being non decreasing, exists t_1 defined by

$$t_1 = \sup\{t' \mid r(t') < t\} = \inf\{t' \mid r(t') > t\}$$

with

$$|t - t_1| < \frac{T_x}{2}$$

Let us consider now the bijective retiming r' such that:

$$\begin{aligned} r'(t - \frac{T_x}{2}) &= t - \frac{T_x}{2} \\ r'(t) &= t_1 \\ r'(t + \frac{T_x}{2}) &= t + \frac{T_x}{2} \end{aligned}$$

and defined by linear interpolation between these points:

$$\begin{aligned} t' \in [t - \frac{T_x}{2}, t] &\Rightarrow r'(t') = t - \frac{T_x}{2} + \frac{t_1 - (t - \frac{T_x}{2})}{\frac{T_x}{2}}(t' - (t - \frac{T_x}{2})) \\ t' \in [t, t + \frac{T_x}{2}] &\Rightarrow r'(t') = t_1 + \frac{t + \frac{T_x}{2} - t_1}{\frac{T_x}{2}}(t' - t) \end{aligned}$$

Clearly $||r' - id|| \leq \varepsilon$ holds over $[t - \frac{T_x}{2}, t + \frac{T_x}{2}]$, and $||x - x \circ r \circ r'||_\infty = 0$ holds on the same interval[3].

Then the proof can proceed by induction on the sequence of discontinuity points of x.

If part: Let us show that if x can have two discontinuity points arbitrarily close, it is not possible to find a value $\eta_x(0.5)$ such that, for any retiming r,

$$||r - id||_\infty \leq \eta_x(0.5) \Rightarrow d_S(x, x \circ r) \leq 0.5$$

Effectively, x must have an unbounded number of couples of discontinuity points closer than $\eta_x(0.5)/2$. There is thus a time t_1 for which this number n_1 of such discontinuity points is larger than $1/\eta_x(0.5)$.

On the other hand, it is easy to construct a retiming r with $||r - id||_\infty \leq \eta_x(0.5)$ which "erases" every couple of discontinuity points closer than $\eta_x(0.5)/2$:

Let t, t' such a couple $t' - \eta_x(0.5)/2 < t < t'$. On can find two other points t'', t''' such that $t'' < t < t' < t''' < t'' + \eta_x(0.5)$ and take:

[3] It may be the case that $x(t) \neq x \circ r \circ r'(t)$ because nothing has been assumed of the value of x at the discontinuity point t. It is here that the concept of equality "almost everywhere" is useful.

$$r(t'') = r(t''') = t''$$

Any bijective retiming $||r' - id||_\infty \leq 0.5$ satisfies according to lemma 2

$$dc_{0,t_1}(x \circ r \circ r') \leq dc_{0,t_1+0.5}(x \circ r)$$

But

$$dc_{0,t_1}(x \circ r) = dc_{0,t_1}(x) - n_1$$

as r erased n_1 discontinuities, and

$$dc_{0,t_1+0.5}(x \circ r) < dc_{0,t_1}(x)$$

as x cannot have n_1 non erasable discontinuities in $[t_1, t_1 + 0.5]$

Thus,

$$dc_{0,t_1}(x \circ r \circ r') < dc_{0,t_1}(x)$$

$$||x - x \circ r \circ r'||_\infty = 1$$

which contradicts the hypothesis

$$d_S(x, x \circ r) \leq 0.5$$

One clearly sees the idea of this theorem: if x has uniform bounded variability, one can find a continuous bounded retiming which has the same effect as a bounded but possibility discontinuous one. On the contrary, if variability is unbounded this is no more possible because a discontinuous retiming can erase discontinuity points which are too close from each other, while a continuous retiming cannot. Then the distance between signals that don't have the same number of discontinuities cannot get smaller than 1.

4.3 Skorokhod distance and $||\ ||_\infty$

As for continuous signals and systems, it is obvious that the Skorokhod distance encompasses the usual $||\ ||_\infty$ one because for any x, y, $d_S(x,y) \leq ||x - y||_\infty$:

Theorem 5. *A uniformly continuous signal is Skorokhod uniformly continuous.*

This clearly shows that the Skorokhod distance can both deal with discontinuous signals, like booleans, and continuous ones. It is thus a good candidate for dealing with mixed cases *i.e.*, systems dealing with both continuous and, say, boolean signals as well as signals which are "piece-wise uniformly continuous".

5 Conclusion and Open Questions

This paper has thus addressed the question of extending the usual approximation and sampling theory of continuous signals and systems to those encompassing discontinuities, such as found in modern complex control systems (mode switches for instance). We have provided some evidence that the Skorokhod topology is a good candidate for dealing with those cases in a uniform manner.

Yet, much remains to do in order to achieve this goal. In particular, two important issues have to be raised here:

Multiple input-output systems: we only treated here the case of single input-output systems. The case of multiple ones is much more involved: what are the systems that are uniformly continuous in their several inputs? Some hints on the subject have been proposed in [5], but not linked with the topological approach followed here.

Links with stability: in fact, even the classical approach presented in section 2 is unsatisfactory, as it only applies to stable systems and it is well-known that many controllers are not stable. For instance the celebrated PID controller is not stable, since it contains an integral part, and hence, it is not uniformly continuous (figure 5). Thus controllers cannot be analysed in isolation of the systems they intend to stabilise and uniform continuity only applies to the closed loop system (figure 6).

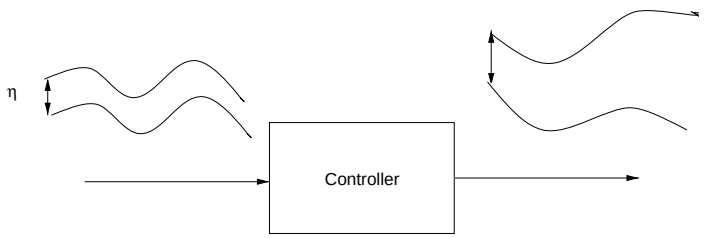

Fig. 5. An unstable system

This problem is likely to arise similarly in our framework and raises the question of stability characterisation and of feed-back stabilisation in the case of mixed continuous-discontinuous signals and systems. In particular, it would be tempting to interpret critical race avoidance and protocols within this framework [4].

Acknowledgments: The authors kindly acknowledge Alberto San Giovanni-Vincentelli from Berkeley University for pointing us reference [9].

References

1. A.Chutinan and B.H.Krogh. Computing approximating automata for a class of hybrid systems. *Mathematical and Computer Modeling of Dynamical Systems*, 6:30–50, March 2000. Special Issue on Discrete Event Models of Continuous Systems. 2

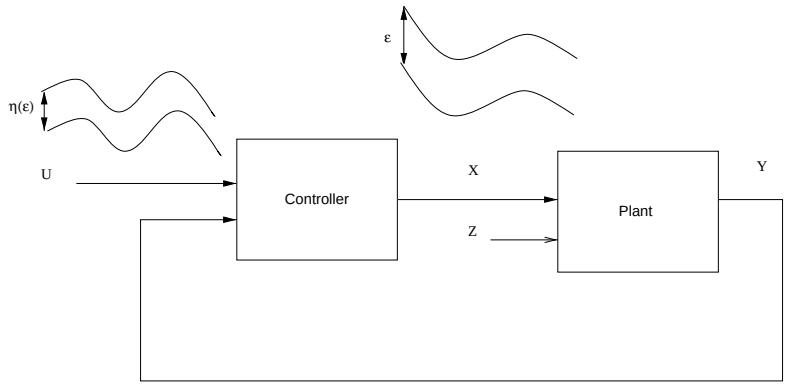

Fig. 6. Feed-back stabilisation

2. P. Billingsley. *Convergence of probability measures*. John Wiley & Sons, 1999. 7
3. M.S. Branicky. Topology of hybrid systems. In *32nd Conference on Decision and Control*, pages 2309–2311. IEEE, 1993. 2
4. P. Caspi. Embedded control: from asynchrony to synchrony and back. In T. Henzinger and Ch. Kirsch, editors, *First International Wokshop on Embedded Software*, volume 2211 of *Lecture Notes in Computer Science*, 2001. 10
5. P. Caspi and R. Salem. Threshold and bounded-delay voting in critical control systems. In Mathai Joseph, editor, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 1926 of *Lecture Notes in Computer Science*, pages 68–81, September 2000. 1, 10
6. E.Asarin, O.Maler, and A.Pnueli. On discretization of delays in timed automata and digital circuits. In R.de Simone and D.Sangiorgi, editors, *Concur'98*, volume 1466 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 1998. 2
7. J.Ouaknine. Digitisation and full abstraction for dense-time model checking. In *TACAS 02*, volume 2280 of *Lecture Notes In Computer Science*, pages 37–51. Springer, 2002. 2
8. H. Kopetz. *Real-Time Systems Design Principles for Distributed Embedded Applications*. Kluwer, 1997. 1
9. M.Broucke. Regularity of solutions and homotopic equivalence for hybrid systems. In *Proceedings of the 37th IEEE Conference on Decision and Control*, volume 4, pages 4283–4288, 1998. 2, 10
10. R.Alur, T.A.Henzinger, G.Lafferriere, and G.J.Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88:971–984, 2000. 2
11. J.H. Wensley, L. Lamport, J. Goldberg, M.W. Green, K.N. Lewitt, P.M. Melliar-Smith, R.E Shostak, and Ch.B. Weinstock. SIFT: Design and analysis of a fault-tolerant computer for aircraft control. *Proceedings of the IEEE*, 66(10):1240–1255, 1978. 1
12. W.Kohn and A.Nerode. Models for hybrid systems: automata, topologies, controllability and observability. In *Hybrid Systems*, volume 732 of *Lecture Notes in Computer Science*. Springer, 1993. 2