



UNIVERSIDADE TÉCNICA DE LISBOA  
INSTITUTO SUPERIOR TÉCNICO

# **CÓDIGOS DE CONTROLO DE ERROS PARA O SISTEMA MBS**

**Paulo Jorge Dias Torres**  
**Licenciado**

**Dissertação para a obtenção do grau de mestre em**  
**Engenharia Electrotécnica e de Computadores**

**Orientador:**

**Prof. Doutor António Manuel de Assis Gusmão Correia**

**Júri:**

**Prof. Doutor António Manuel de Assis Gusmão Correia**

**Prof. Doutor Victor Manuel Paulino Vargas**

**Prof. Doutor Luís António Serralva Vieira de Sá**

**Julho de 1996**

Tese realizada sob a orientação de

António Manuel Gusmão Correia

Professor Auxiliar do

Departamento de Engenharia Electrotécnica e de Computadores

INSTITUTO SUPERIOR TÉCNICO

# Resumo

O objectivo do sistema MBS (Mobile Broadband System), actualmente objecto de pesquisa na Europa, no âmbito do projecto RACE R2067/MBS, é disponibilizar aos utilizadores móveis um acesso rádio de base ATM à futura rede de banda larga (IBCN). A implementação de um interface rádio para o sistema MBS não é tarefa simples, uma vez que as condições de propagação tornam os canais disponíveis bastante adversos à radiotransmissão (ritmos altos de transmissão sobre portadoras na banda das ondas milimétricas), e os objectivos dos serviços são ambiciosos (por exemplo: probabilidades de erro abaixo de  $10^{-6}$  com atrasos de alguns milissegundos).

Esta tese dedica especial atenção ao contributo de códigos de controlo de erros para bons compromissos entre qualidade do serviço e requisitos de potência de emissão.

No início da tese, é descrito o interface rádio do sistema MBS (características e parâmetros principais), fazendo-se também referência às limitações e requisitos de transmissão. É apresentado em seguida o esquema de controlo de erros escolhido, baseado na concatenação de um código interno convolucional com rendimento  $3/4$  e de um código externo construído sobre um campo finito  $GF(2^6)$ , que é um código RS(60,36) encurtado. Trata-se de um esquema híbrido (ARQ/FEC), muito flexível, desenhado para combinar capacidades de detecção e correcção de erros de um modo adaptativo; quando solicitado, é possível enviar um *burst* médio, com redundância adicional (para aumentar a capacidade de controlo de erros), em alternativa à retransmissão convencional. A operação do esquema de controlo de erros proposto é dependente de um limiar que é estabelecido de uma forma flexível, de acordo com os requisitos e as características do serviço, e, possivelmente, o estado do canal.

Para finalizar a tese, são discutidos os resultados de desempenho num determinado cenário de simulação. Estes resultados demonstram claramente que o esquema de controlo de erros proposto é poderoso e flexível, podendo ser adaptado a uma variada gama de serviços e características do canal, e é uma contribuição importante para o desenvolvimento de um sistema eficiente.

**Palavras Chave:** Sistema MBS (Mobile Broadband System), Qualidade de Serviço, Requisitos de Potência de Emissão, Códigos de Controlo de Erros, Códigos Reed-Solomon.

# Abstract

The aim of MBS (Mobile Broadband System), currently under research in Europe within the RACE project R2067/MBS, is to offer to mobile users an ATM-based radio access to the future IBCN. The design of an air interface for MBS is not an easy task, since the available propagation channels are very hostile to radio transmission (high data rates over mm-wave carriers) and the service targets are quite ambitious (for example, bit error rates below  $10^{-6}$  with a delay of a few milliseconds).

This thesis is concerned to the contribution of error control coding schemes for better trade-offs between quality of service and transmit power requirements.

To begin with, a brief description of the MBS air interface (main characteristics and parameters) is made, and the main radio transmission requirements and constraints are reported. Next, we present the chosen error control scheme, based on the concatenation of an inner convolutional code with rate  $3/4$  and an outer code, constructed over the Galois field  $GF(2^6)$ , which is a  $(60,36)$  shortened Reed-Solomon (RS) code. It is a very flexible, hybrid, FEC/ARQ scheme, designed to combine error-correction and error detection features in an adaptive manner; it is possible to send, under request, a special medium-size burst with additional redundancy (for increased error correction capabilities), as well as conventional retransmissions. The operation of the proposed error control scheme is "threshold dependent": appropriate thresholds can be established in a flexible way, taking into account service characteristics and requirements, and, possibly, channel state conditions.

To finish the thesis, a set of performance results is shown and discussed, for a given simulation scenario. These results clearly demonstrate that the proposed error control scheme is both powerful and flexible, can be matched to a wide range of services and channel characteristics, and is a key contribution for an efficient system design.

**Keywords:** Mobile Broadband System, Quality of Service, Transmit Power Requirements, Error Control Coding, Reed-Solomon Codes.

## AGRADECIMENTOS

Quero exprimir o meu agradecimento a todos os que contribuíram, directa ou indirectamente, para a realização desta tese. Em particular desejo agradecer,

Ao Professor António Gusmão Correia, meu orientador, pelo tema proposto, pelo incentivo e conhecimentos que me transmitiu, pelas condições de trabalho que me proporcionou e pelo empenho e disponibilidade com que acompanhou todo o meu trabalho.

Aos meus colegas Rui Dinis e Carlos Caseiro, do CAPS, e José Fernandes, da Universidade de Aveiro, pelo *software* que me disponibilizaram, facilitando e enriquecendo esta tese.

Ao meu colega Victor Gonçalves por todo o incentivo dado nas mais diversas alturas do percurso deste trabalho.

Aos meus colegas e amigos do Centro de Análise e Processamento de Sinais (CAPS) pelo excelente ambiente de trabalho e por toda a ajuda que me deram.

À minha madrinha, por toda paciência que teve no decorrer da realização deste trabalho.

À Bibi por todo o apoio que me deu, sem o qual este trabalho não teria sido possível.

Às Paulinhas, pela forma como compreenderam, incentivaram e apoiaram todo o meu empenho neste trabalho.

**Às Paulinhas**

# Índice Geral

1. Introdução	1
1.1. Objectivos do trabalho	1
1.2. Organização da tese	3
2. Interface rádio e problemas de transmissão no sistema MBS	4
2.1. Especificações do interface rádio	4
2.2. Requisitos e restrições a nível de transmissão	8
3. Codificação de canal e procedimentos de controlo de erros no sistema MBS	13
3.1. Controlo de erros com códigos concatenados	15
3.2. Códigos interno e externo	20
3.2.1. Código interno	20
3.2.1.1. Codificação	20
3.2.1.2. Descodificação	22
3.2.2. Código externo	25
3.2.2.1. Construção de $GF(2^6)$ e definição de símbolos RS $2^6$ -ários	27
3.2.2.2. Codificação externa	29
3.3. Descodificação externa	31
3.3.1. Introdução	32
3.3.2. Descrição do código RS usando transformadas de Fourier discretas	33
3.3.3. Algoritmo de Berlekamp-Massey	35
3.3.4. Adaptação do algoritmo de Berlekamp-Massey para correcção de erros e rasuras	40

4. Avaliações de desempenho	45
4.1. Condições de simulação	46
4.1.1. Cenário de simulação	46
4.1.2. Opções de implementação quanto a igualização e diversidade	48
4.1.3. Metodologia de simulação	48
4.2. Resultados numéricos	50
4.3. Discussão dos resultados obtidos	57
5. Conclusões e perspectivas de trabalho futuro	61
<b>Bibliografia</b>	64
<b>Anexo</b>	
A 1. Código RS(7,3) construído sobre GF(2 <sup>3</sup> )	66
A 2. Descodificação	67
A 2.1 Primeiro exemplo de descodificação	67
A 2.2 Segundo exemplo de descodificação	69
A 2.3 Terceiro exemplo de descodificação	71

# Índice de figuras

Figura 2.1: Sistema MBS: Conceito (A) e Aplicações (B).

Figura 2.2: Estrutura da trama e respectivos *bursts*.

Figura 2.3: Configurações celulares para ambientes interiores (A) e exteriores (B).

Figura 2.4: Exemplo de distribuições cumulativas da potência recebida (A) e do *delay spread* (B).

Figura 2.5: Exemplo de distribuições cumulativas dos erros.

Figura 3.1: Papel dos códigos concatenados na construção dos *bursts standard* e médio.

Figura 3.2: Fluxograma do esquema de controlo de erros.

Figura 3.3: Codificador convolucional.

Figura 3.4: *Trellis* do código convolucional perfurado.

Figura 3.5: Par de sequências de código distando  $d_t=4$ .

Figura 3.6: Ilustração de um “acontecimento de erro” abarcando seis ramos.

Figura 3.7: Circuito linear associado ao algoritmo de Berlekamp Massey.

Figura 3.8: Descodificador de Berlekamp Massey.

Figura 4.1: Cobertura da BS no cenário de simulação.

Figura 4.2: Parâmetros de dispersão (*delay spread*)

Figura 4.3: Desempenho do DFE com as seguintes antenas:

- Antena omnidireccional com polarização vertical.
- Antena omnidireccional com polarização circular.
- Antena directiva com polarização vertical.

Figura 4.4: Desempenhos para diferentes limiares e antenas.

Figura 4.5: Desempenhos para os seguintes casos:

- Antena omnidireccional com polarização vertical a 100m da BS.
- Antena omnidireccional com polarização circular a 100m da BS.
- Antena directiva com polarização vertical a 100m da BS.
- Antena directiva com polarização vertical a 240m da BS.

Figura 4.6: Fluxograma dum esquema de controlo de erros sem utilização de limiares externos.

Figura 4.7: Desempenhos sem utilização de limiares externos.

## LISTA DE ABREVIATURAS

- ARQ - Automatic Repeat ReQuest
- ACK - Positive Acknowledgement
- ATM - Assynchronous Transfer Mode
- BCH - Bose Chaudhuri-Hocquenghem
- BER - Bit Error Rate
- B-ISDN - Broadband Integrated Services Digital Network
- BS - Base Station
- DFE - Decision Feedback Equalizer
- DFT - Discrete Fourier Transform
- FDD - Frequency Division Duplexing
- FDMA - Frequency Division Multiple Access
- FEC - Forward Error Correction
- GBR - Gross Bit Rate
- GSM - Global System for Mobile Communications
- IBCN - Integrated Broadband Communication Network
- IDFT - Inverse Discrete Fourier Transform
- MAC - Medium Access Control
- MBS - Mobile Broadband System
- MS - Mobile Station
- NAK - Negative Acknowledgement
- OQAM - Offset Quadrature Amplitude Modulation
- RF - Radio Frequency
- RS - Reed-Solomon

SBR - Service Bit Rate

TDMA - Time Division Multiple Access

UMTS - Universal Mobile Telecommunications System

# Capítulo 1

## INTRODUÇÃO

### *1.1 Objectivos do trabalho*

Este trabalho foi realizado no âmbito de um projecto europeu na área das comunicações móveis: trata-se do projecto RACE 2067/MBS (Mobile Broadband System), que vem estudando a viabilidade dum sistema capaz de oferecer a utilizadores móveis um acesso rádio, de base ATM, à futura IBCN (Integrated Broadband Communication Network [1]. O desenvolvimento deste sistema constitui um desafio considerável, sendo imprescindível um alto grau de flexibilidade (grande variedade de serviços e ambientes de funcionamento) e a possibilidade de uma implementação de baixo custo (ainda que com capacidades reduzidas) num futuro próximo, com a posterior incorporação de capacidades adicionais de acordo com o progresso tecnológico.

Os objectivos desta tese têm a ver com os requisitos de qualidade/potência no âmbito daquele sistema, particularmente difíceis de satisfazer: devido às características de muitos dos serviços previsíveis, que podem exigir, por exemplo, probabilidades de erro não superiores a  $10^{-6}$ , com atrasos de apenas alguns milisegundos; devido aos altos débitos de transmissão necessários, sobre portadoras na banda das ondas milimétricas (a banda larga que o sistema requer não está disponível abaixo dos 30GHz).

As actividades desenvolvidas no âmbito do projecto MBS com vista à caracterização dos canais de propagação mostraram claramente que aquela depende fortemente das escolhas feitas no tocante às antenas e às configurações celulares: por exemplo, uma certa directividade (quer no plano horizontal, quer no plano vertical) ajuda a evitar valores demasiado elevados do “delay spread”, permitindo bons desempenhos com igualizadores e esquemas de diversidade de complexidade reduzida

[2,3]; além disso, as antenas directivas permitem reduzir os níveis de potência de emissão, sendo no entanto de referir que a respectiva implementação para terminais móveis não é simples, pois terão que ser, de alguma maneira, adaptativas.

Esta tese é especialmente dedicada ao contributo de códigos de controlo de erros, projectados tendo em conta as características e parâmetros específicos do sistema MBS, para bons compromissos entre qualidade de serviço e nível de potência transmitida. Procurou-se que o método de controlo de erros a desenvolver, além de minimizar os requisitos de potência para níveis especificados de qualidade de serviço, possuisse características de flexibilidade que o tornassem adequado para uma gama ampla de serviços, com características muito diversas, e para variados ambientes de transmissão e “estados” do canal.

A estratégia de controlo de erros proposta baseia-se numa concatenação de códigos, com um código convolucional como código interno e um código de blocos não binário, da “classe Reed-Solomon”, como código externo. A avaliação dos desempenhos proporcionados por esta estratégia implicou simulações de Monte-Carlo para as quais o autor teve à sua disposição *software* desenvolvido no âmbito do Grupo de Comunicação Digital do CAPS (igualização por realimentação de decisões e descodificação de códigos convolucionais com o algoritmo de Viterbi) e do Grupo de Micro-ondas da Universidade de Aveiro (simulação de efeitos de propagação com uma ferramenta de “Ray-tracing”). Alguns dos resultados preliminares deste trabalho foram já objecto de publicação [4].

## **1.2 Organização da tese**

A presente tese encontra-se dividida em cinco capítulos e um anexo.

A seguir ao presente capítulo introdutório, faz-se no capítulo 2 a descrição das especificações do interface rádio do sistema MBS e referem-se os principais requisitos e restrições a nível da transmissão no âmbito desse sistema.

No capítulo 3 é proposta uma estratégia tendo em conta a estratégia de controlo de erros para o sistema MBS.

No capítulo 4 é feita a respectiva avaliação de desempenho num cenário típico de transmissão em ambiente exterior. As conclusões do presente trabalho e as perspectivas para a sua continuação são apresentadas no capítulo 5.

# Capítulo 2

## INTERFACE RÁDIO E PROBLEMAS DE TRANSMISSÃO NO SISTEMA MBS

### *2.1 Especificações do interface rádio*

A implementação de um sistema celular, capaz de oferecer a utilizadores móveis um acesso rádio, de base ATM (Assynchronous Transfer Mode), à futura rede de banda larga IBCN (B-ISDN: Broadband-Integrated Services Digital Network), representa certamente um desafio considerável:

- A gama de serviços é muito ampla, com uma grande variedade de características e requisitos (Ver figura 2.1), incluindo ritmos acima de 100Mbps, muito superiores aos usados nos sistemas de rádio móvel correntes, como o GSM, e outros sistemas a introduzir num futuro próximo (UMTS: Universal Mobile Telecommunications System). Além disso, em alguns casos, com probabilidades de erro e atrasos toleráveis muito inferiores.
- É necessário recorrer às ondas milimétricas para efeitos de radiotransmissão, uma vez que os elevados ritmos requeridos implicam uma banda muito larga para o sistema (não disponível abaixo dos 30GHz); isto levanta problemas, alguns ainda por resolver, ligados às condições de propagação e à tecnologia de micro-ondas disponível, agravados pela obrigatoriedade de transmitir sinais de banda larga, bastante vulneráveis ao "delay spread".

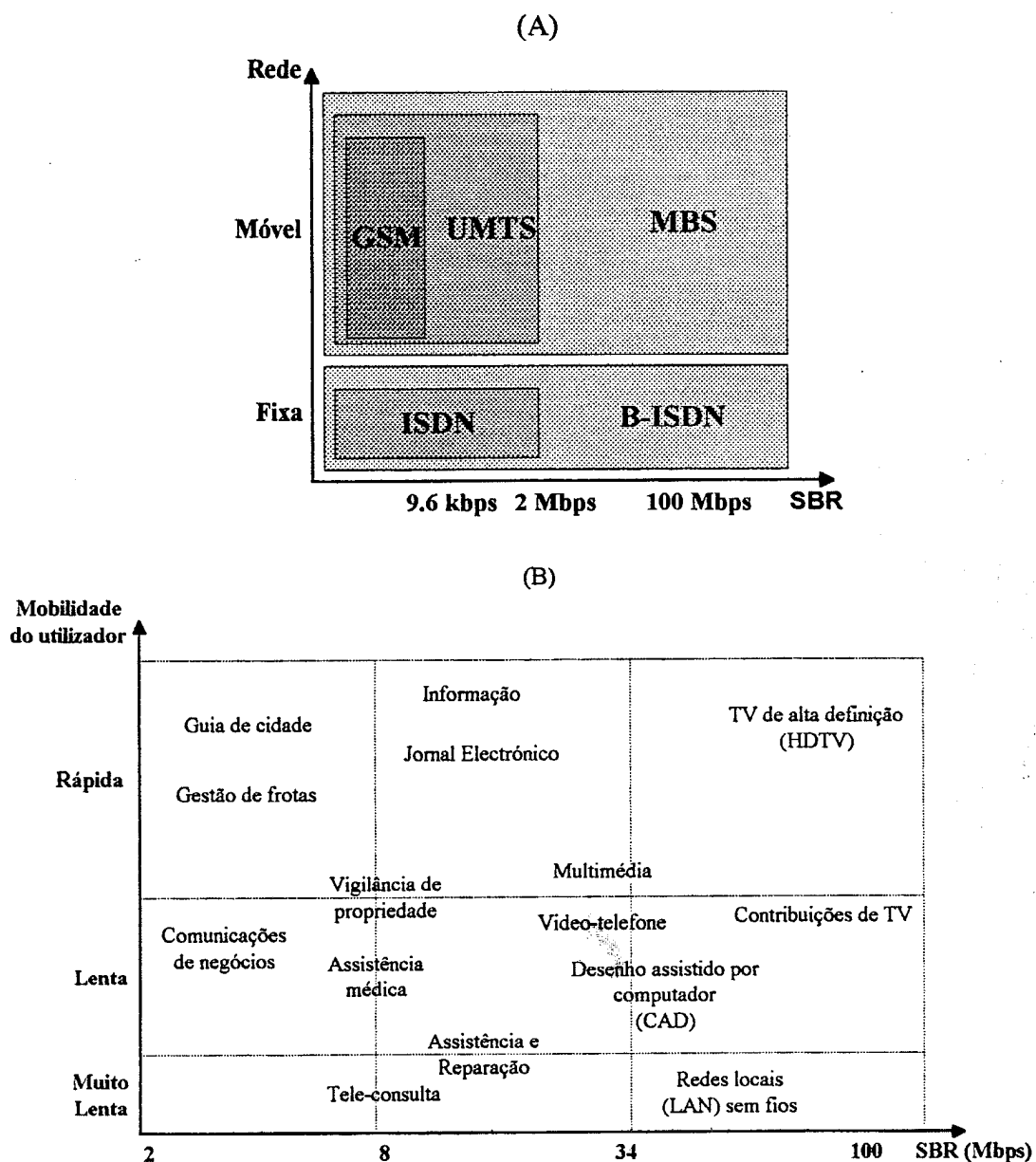


Figura 2. 1: Sistema MBS: Conceito (A) e Aplicações (B).

No âmbito do projecto MBS, foram estabelecidos à partida os seguintes princípios básicos, no que diz respeito ao interface rádio [1,5]:

- Uma das bandas disponíveis (62-63 e 65-66 GHz) é usada para a ligação ascendente e a outra para a ligação descendente, possibilitando a transmissão e recepção simultâneas (FDD: Frequency Division Duplexing).
- Adopta-se um esquema híbrido de acesso múltiplo, por divisão no tempo e na frequência (TDMA/FDMA: Time Division Multiple Access /Frequency

Division Multiple Access); o número de slots ocupados por trama depende do ritmo inerente ao serviço pretendido, podendo mesmo utilizar-se praticamente toda a trama; para os ritmos mais elevados, poderão ser usadas várias (até quatro) portadoras em paralelo.

- Cada *burst standard* transporta a informação inerente a uma célula ATM (opção ATM-1) ou duas células ATM (opção ATM-2).
- Podem ser utilizados dois métodos de modulação (4-OQAM e 16-OQAM: Offset Quadrature Amplitude Modulation), ambos com o mesmo *symbol rate* para cada tipo de ambiente: interior (*indoor*) e exterior (*outdoor*); os métodos de modulação 4-OQAM e 16-OQAM estão relacionados, respectivamente, com as opções ATM-1 e ATM-2 para cada modulação; o ritmo bruto (GBR - Gross Bit Rate) em ambientes interiores é o dobro do adoptado em ambientes exteriores.
- Numa fase inicial da implementação do sistema, só se prevê a utilização da modulação 4-OQAM (e portanto da opção ATM-1), com baixa flutuação de envolvente; isto deve-se a dificuldades, ainda não superadas, no que diz respeito à amplificação de potência na banda das ondas milimétricas (mesmo sendo fortemente não-lineares, os amplificadores já realizados exibem rendimento muito baixo).

Algumas das especificações previstas para o interface rádio, numa primeira fase de implementação do sistema (opção ATM-1 em todas as situações) e para operação em ambientes exteriores, são indicadas em seguida (Ver Fig. 2-2):

- 40 *slots standard* por trama, sendo  $19.2\mu\text{s}$  a duração de cada slot e  $40 \times 19.2 = 768\mu\text{s}$  a duração da trama;
- Duração do *burst standard* igual a  $17.8\mu\text{s}$ , pois é necessário um "tempo de guarda" de  $19.2 - 17.8 = 1.4\mu\text{s}$ .
- 712 bits por *slot standard*, sendo 40 para uma sequência de treino e duas *tails*, localizadas no centro e nas extremidades do *burst*, respectivamente; os  $712 - 40 = 672$  bits restantes traduzem informação codificada, correspondente

à célula ATM (384 bits de tráfego mais 40 bits de cabeçalho) e a bits de controlo (8 bits).

- Ritmo bruto de transmissão  $GBR = \frac{712}{17.8} = \frac{328}{8.2} = 40\text{Mbps}$ .
- *Bursts* médios, desenhados para ocupar *slots* médios, (com metade da duração; nos  $\frac{19.2}{2} - 1.4 = 8.2\mu\text{s}$  de duração destes *bursts* estão contidos  $40 \times 8.2 = 328$  bits; dos quais  $328 - 40 = 288$  bits restantes traduzem informação codificada, designadamente em conformidade com a estratégia de controlo de erros proposta no capítulo 3 desta tese.

Estas especificações implicam um ritmo útil de informação (SBR) máximo por portadora (se todos os *slots standard* de cada trama fossem ocupados por *bursts standard*) é  $SBR = \frac{384 \times 40}{768} = 20\text{Mbps}$ . Isto significa que o objectivo pretendido de 17Mbps [1] pode ser alcançado, se os *slots standard* ocupados com transmissões adicionais (para controlo de erros, procedimentos de sinalização, etc.) representarem menos de 15% da trama.

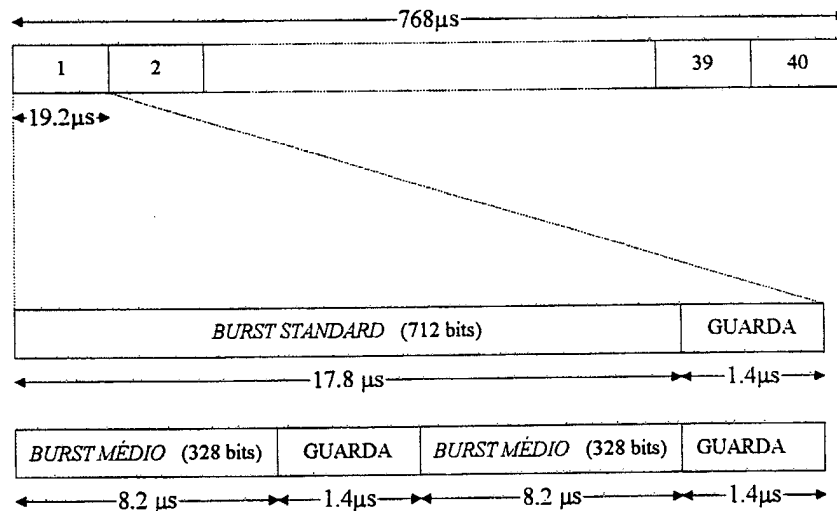


Figura 2. 2: Estrutura da trama e respectivos *bursts*.

## 2.2 Requisitos e restrições a nível de transmissão

O impacto da propagação multipercurso em sinais de banda larga como os requeridos pelo sistema MBS envolve, quer a distorção daqueles sinais, quer o desvanecimento (*fading*) das respectivas envolventes: trata-se de um desvanecimento selectivo na frequência, cujos efeitos podem ser mitigados pelo emprego de técnicas de diversidade espacial, em associação com técnicas de igualização adaptativa. Durante os últimos anos, foi realizado no âmbito do projecto MBS muito trabalho de simulação da transmissão (até ao início da preparação desta tese sem incluir o impacto dos códigos de controlo de erros); os resultados obtidos sugerem a razoabilidade de especificações do interface rádio como as referidas na secção 2.1, pois permitem desempenhos aceitáveis mesmo com técnicas de igualização/diversidade de complexidade reduzida [2]; verificou-se ainda que o desempenho é fortemente condicionado pelas características das antenas (diagrama de radiação, polarização, localização e orientação), no âmbito das estruturas celulares escolhidas [3,6]. Técnicas de "ray-tracing" [7], convenientemente adaptadas tanto a ambientes interiores como exteriores, foram utilizadas no sentido de obter dados de propagação para avaliação dos desempenhos da radiotransmissão, por simulação de Monte-Carlo, incluindo o impacto das diversas opções em matéria de antenas e estruturas celulares [3,6].

De um modo geral, verificou-se serem recomendáveis antenas muito directivas nas estações de base, em ambientes exteriores (ruas de cidade, por exemplo) em que se pretenda alcances superiores a duzentos metros. Veja-se, a propósito, a estrutura celular indicada na figura 2.3, em que a área sob uma dada estação de base é coberta pelas estações de base vizinhas. Este tipo de estrutura permite compatibilizar bons desempenhos com potências de emissão relativamente baixas, o que é muito importante a nível das estações móveis, dependentes de baterias. Tem ainda duas outras características positivas: contribui para um *delay spread* suficientemente baixo para permitir bons desempenhos, numa transmissão a 40 Mbps (ver secção 2.1), mesmo com baixa complexidade de igualização/diversidade; contribui para diminuir a probabilidade de quebra da ligação por interrupção do raio directo (uma questão crucial em ambientes exteriores), pois qualquer ponto da rua é coberto por duas estações de base.

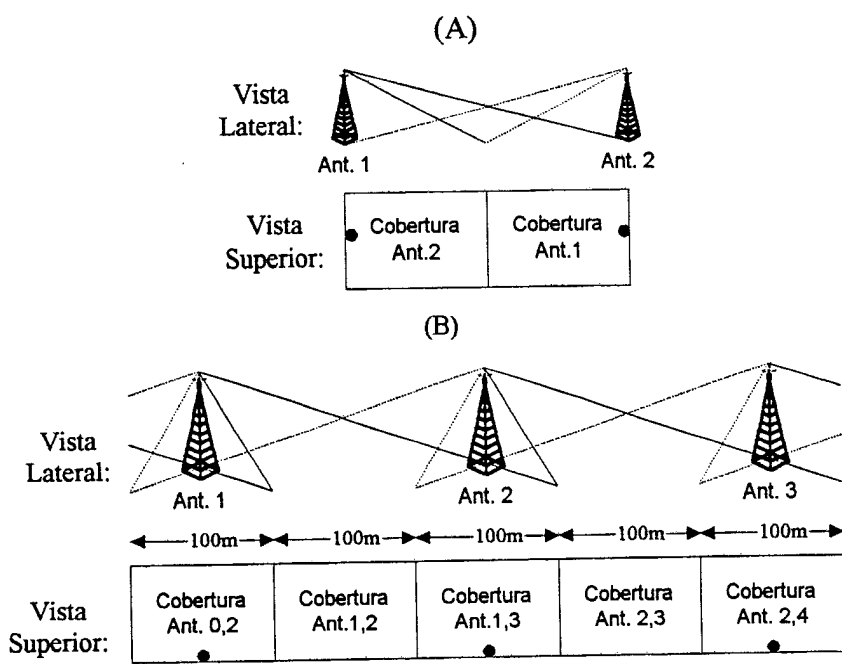


Figura 2. 3: Configurações celulares para ambientes interiores (A) e exteriores (B).

Em ambientes interiores não é tão crítico o emprego de antenas directivas nas estações de base; isto é especialmente verdade para salas de pequenas dimensões, em que a cobertura com antena omnidireccional centralizada produz resultados satisfatórios para os 80 Mbps previstos (ver secção 2.1). No entanto, para uma sala de maiores dimensões é recomendável adoptar uma estrutura de duas células, com antenas directivas em cada estação de base, e cobrindo directamente a metade oposta da sala; é a situação que a figura anterior ilustra, e que é abordada em [6]. Note-se ainda que, em ambientes interiores, não é tão crítica como em ambientes exteriores a ausência de raio directo, pois há tipicamente raios reflectidos com potência suficiente para assegurar a continuação da ligação quando aquele é interrompido.

Quanto às antenas a usar nas estações móveis, uma certa directividade no plano horizontal parece ser dispensável em ambientes interiores, mas o mesmo não se pode dizer relativamente a muitos ambientes exteriores [3]. A dificuldade de implementar a directividade nas antenas dos móveis é, contudo, inegável, devido ao problema da orientação das mesmas de modo a "seguir" a estação de base. Quaisquer antenas capazes de exibir directividade horizontal deverão ser adaptativas, seja sob a forma de esquemas de feixes comutáveis, seja sob a forma de agregados (arrays) de múltiplas

antenas elementares; uma directividade muito elevada poderia, na prática, tornar dispensável a igualização, mas seria sempre de difícil implementação, em especial se pretendêssemos garantir a ligação para as velocidades mais elevadas em zonas urbanas, devido às grandes capacidades de seguimento então requeridas.

No capítulo 4 desta tese são apresentados e comentados resultados de simulação relativos a uma transmissão em ambiente exterior, idêntico ao considerado em [3]. Estes resultados permitem avaliar o impacto do esquema de controlo de erros proposto no capítulo 3 e também, de alguma maneira, avaliar mais completamente e de forma articulada as opções em matéria de antenas e diversidade/igualização.

Para já importa referir a variabilidade do canal de transmissão no domínio do tempo: as condições de transmissão são tipicamente, bastante boas para a maior parte dos *slots* e só durante uma pequena percentagem destes as referidas condições se degradam. A título de exemplo, mostram-se na figura 2.4 as distribuições cumulativas da potência recebida (A) e do *delay spread* (B), para uma das hipóteses de implementação (antena de feixes comutáveis na MS), no âmbito do cenário atrás citado. Nessas condições, e para um esquema de diversidade espacial dupla por selecção da máxima potência e um igualizador com realimentação das decisões (DFE), verificam-se as distribuições de erros que a figura 2.5 mostra nas decisões do DFE. Nesta figura, os valores médios correspondentes da taxa de erros são, respectivamente,  $10^{-2}$  (A),  $2.5 \times 10^{-3}$  (B) e  $7 \times 10^{-4}$  (C); muitos *bursts* têm um baixo número de erros, ou mesmo nenhum, e só se obteve um elevado número de erros para uma pequena percentagem dos *bursts* simulados. Note-se, contudo, que as distribuições de erros são bastante dependentes de  $\bar{E}_b/N_0$  ( $\bar{E}_b$  designa a energia média por bit e  $N_0$  a densidade espectral de potência do ruído gaussiano equivalente na entrada do receptor), sendo claro que, para valores baixos de  $\bar{E}_b/N_0$ , a percentagem de *bursts* “maus” e “péssimos” tende a tornar-se muito significativa. A variabilidade no tempo do canal de transmissão, traduzida por distribuições de erros como as aqui exibidas, é um elemento importante a ter em conta para o desenvolvimento de um método apropriado de controlo de erros, o que será feito no capítulo seguinte.

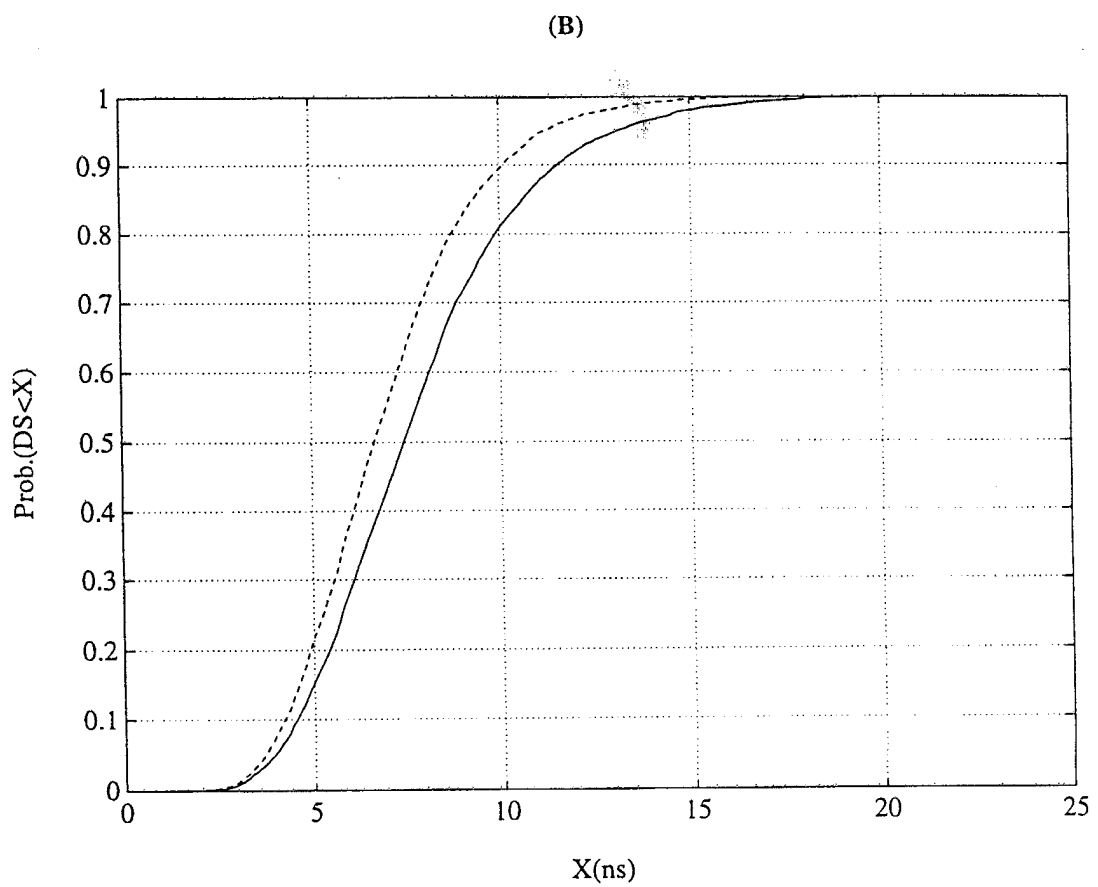
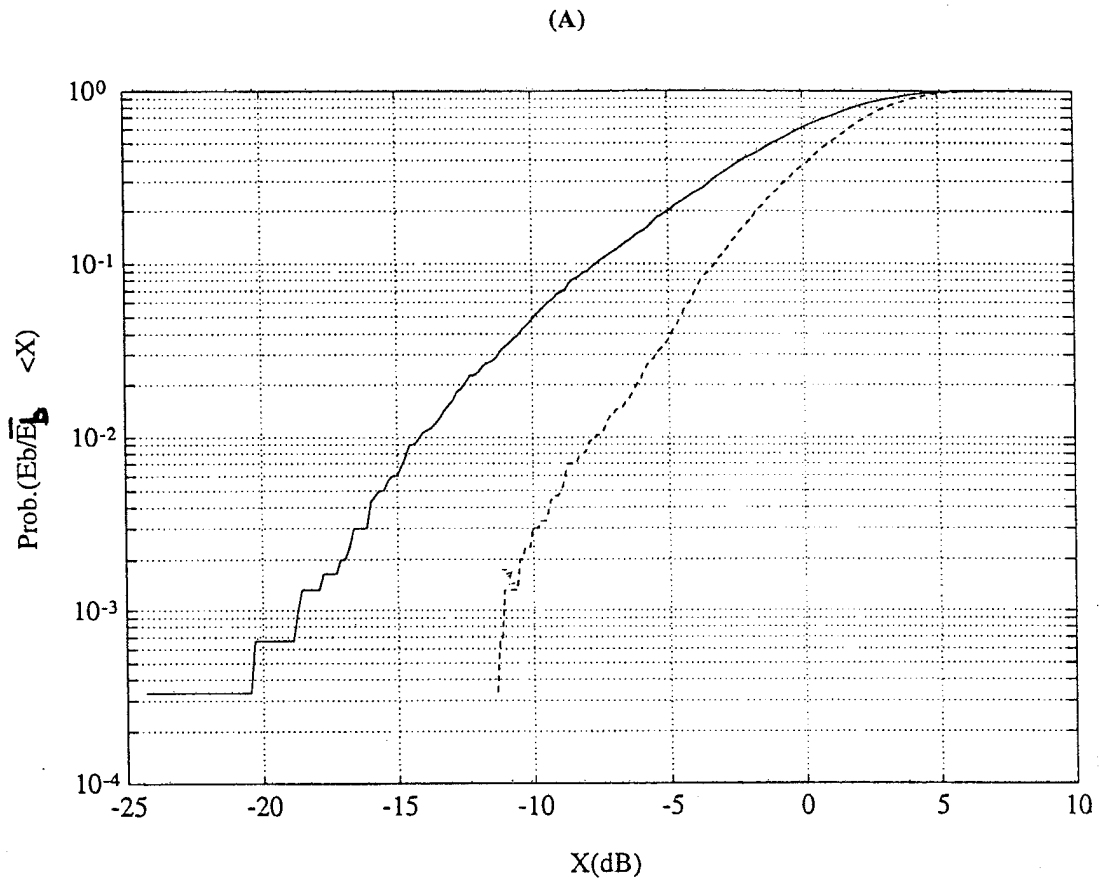


Figura 2.4: Exemplo de distribuições cumulativas da potência recebida (A) e do *delay spread* (B), sem diversidade (\_\_\_\_) e com diversidade (-----).

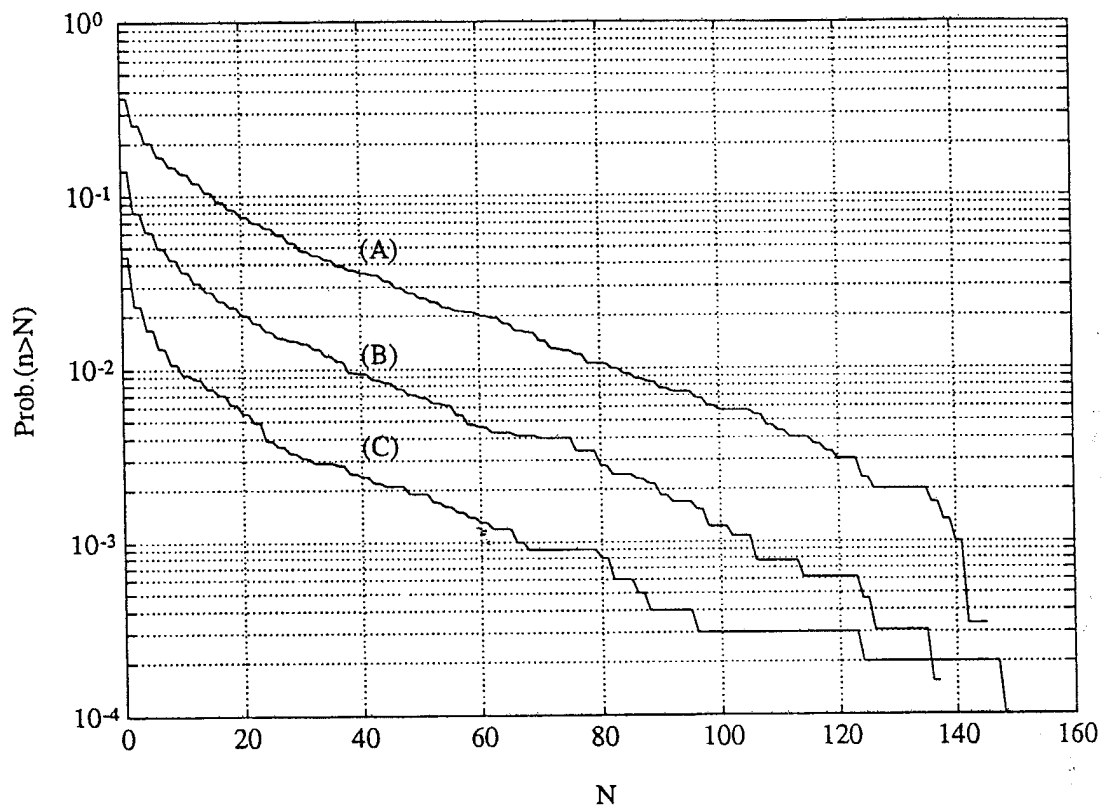


Figura 2. 5: Exemplo de distribuições cumulativas dos erros ( $n$ : número de erros à saída do igualizador por *burst standard*):  $\frac{\bar{E}_b}{N_0} = 7\text{dB}$  (A),  $\frac{\bar{E}_b}{N_0} = 10\text{dB}$  (B),  $\frac{\bar{E}_b}{N_0} = 13\text{dB}$  (C).

# Capítulo 3

## CODIFICAÇÃO DE CANAL E PROCEDIMENTOS DE CONTROLO DE ERROS NO SISTEMA MBS

A existência de ruído num canal não impossibilita a transmissão de informação com baixas probabilidades de erro. Contribui para este objectivo a codificação de canal, que, através da introdução de redundância na sequência de símbolos transmitida, permite um efectivo controlo de erros (detecção e/ou correcção), e, por via desse controlo, melhora a qualidade de serviço. O emprego de códigos de controlo de erros não só aumenta a fiabilidade da transmissão, como também permite reduzir os níveis de potência necessários.

Para canais estáveis, com qualidade boa ou média, pode utilizar-se a estratégia de controlo de erros convencional ARQ (Automatic Repeat Request) [8], geralmente eficiente mesmo com pouca redundância; no entanto, para más condições de transmissão, o número de repetições (na sequência de detecção de erros) pode tornar-se excessivo. Como alternativa, existe a estratégia FEC (Forward Error Correction) convencional, especialmente adequada para o controlo dos erros em canais com características conhecidas e praticamente invariantes no tempo. Contudo, em situações de variabilidade do canal, a capacidade correctora mostra-se desnecessária durante grande parte do tempo, e nos pequenos períodos em que o canal está em “mau estado”, pode, pelo contrário, mostrar-se insuficiente. Como solução, utiliza-se normalmente, com desempenhos satisfatórios, um esquema de *interleaving* profundo (envolvendo vários *bursts* no caso dos sistemas TDMA) para espalhar os erros e obter uma distribuição mais ou menos uniforme dos mesmos à entrada do decodificador; é o que sucede no sistema GSM. Uma solução poderosa para aplicações FEC, bem conhecida, é a concatenação de um código convolucional interno (com decodificação assente em decisões brandas) com um código externo Reed-Solomon [9,10,11]. A

qualidade do serviço tem a ver quer com a probabilidade de erro residual uma vez completada a descodificação (isto é, com a fiabilidade da transmissão de informação) quer com o atraso inerente a esta; neste sentido, tanto o excesso de repetições (ARQ) como um *interleaving* demasiado profundo (FEC) podem significar uma qualidade de serviço inaceitável, mesmo quando é atingida uma probabilidade de erro residual bastante baixa.

Se se combinarem as estratégias ARQ e FEC, sob uma forma híbrida, pode obter-se um bom equilíbrio entre atraso, fiabilidade da transmissão e taxa de débito efectiva, esta última função da taxa de retransmissões necessárias. Este é o caso do esquema “híbrido do tipo II” [12], que usa um código de correcção de erros invertível, com rendimento 1/2, que só requer a transmissão de redundância para a correcção dos erros quando isso se torna necessário; as sequências de “informação” e de “paridade” (redundância) podem ser utilizadas para detectar a presença de erros e, nesse caso, são combinadas para conferir ao código uma capacidade de correcção de erros suficiente. Outra possibilidade interessante é enviar sucessivos dígitos de paridade para construir um código que seja suficientemente poderoso para o sucesso da descodificação (diferentemente do que sucede no esquema “híbrido do tipo II”, atrás mencionado, não são repetidos dígitos antes transmitidos [13]). Este esquema “ARQ/FEC híbrido” pode ser visto como um esquema de controlo de erros adaptativo, sendo especialmente interessante para aplicações em que o canal é variável no tempo, como sucede nas comunicações móveis; isto deve-se à sua capacidade para adaptar a redundância do código ao estado do canal.

Na secção 3.1 deste capítulo é apresentada uma estratégia de controlo de erros para o sistema MBS: trata-se de uma estratégia híbrida, ARQ/FEC, assente numa concatenação de códigos (um código convolucional interno e um código de blocos externo), compatível com as especificações do interface rádio daquele sistema e adaptada às respectivas condições de transmissão (ver capítulo 2), bem como às características do modo de transmissão ATM e de uma ampla gama de serviços [14]. Quer o código interno quer o externo são caracterizados na secção 3.2. A secção 3.3 é especialmente dedicada ao código externo, incluindo a descrição detalhada de um algoritmo de descodificação.

### 3.1 Controlo de erros com códigos concatenados

A estratégia de controlo de erros que propomos para o sistema MBS é baseada na concatenação de um código interno convolucional, com ritmo 3/4, e de outro externo, construído sobre o campo finito  $GF(2^6)$ , que é um código “Reed-Solomon encurtado” RS(60,36). Como vimos na secção 2.1, assumiu-se que dos 54 octetos (72 sextetos) de bits de informação transportados por um *burst standard*, apenas 48 são inerentes ao serviço em causa; dos restantes 6 octetos, 5 correspondem ao cabeçalho (*header*) da célula ATM e o octeto suplementar inclui sinalização específica do interface rádio. O conteúdo útil de cada *burst standard* é construído da seguinte forma: com base nos 72 sextetos acima citados, obtêm-se duas palavras de um código RS(42,36), definido por “perfuração” (*puncturing* [10]) do código RS(60,36); o bloco de bits correspondente a estas palavras (504 bits) é submetido ao codificador interno, obtendo-se os 672 bits referidos na secção 2.1. No caso de o decodificador o solicitar, é enviado o *burst médio* (288 bits), com base no par de 60-42=18 sextetos de paridade anteriormente retidos, depois de devidamente submetidos ao codificador interno.

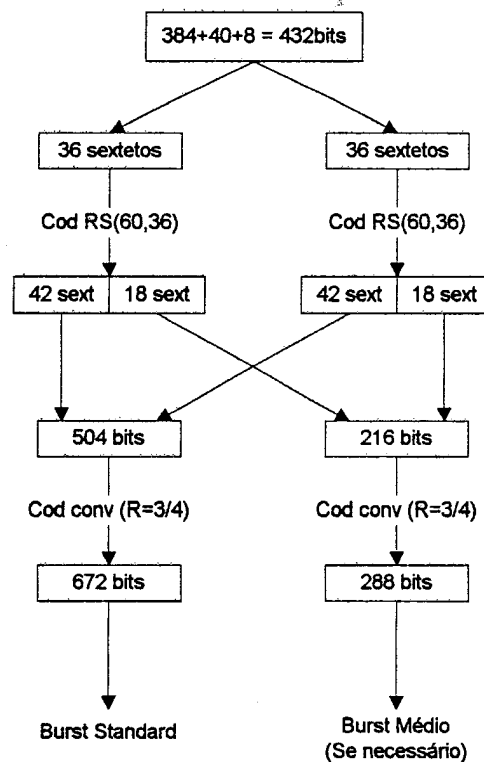


Figura 3. 1: Papel dos códigos concatenados na construção dos *bursts standard* e médio.

A estratégia de controlo de erros proposta é uma estratégia híbrida ARQ/FEC bastante flexível, combinando capacidades de correcção e detecção de erros de forma adaptativa. Enunciam-se a seguir alguns dos seus pressupostos:

- Não requer *interleaving* entre *bursts*, dado que não se trata de FEC puro; todavia é recomendável o emprego de *interleaving* no interior de cada *burst*, a nível dos símbolos de modulação, pois se verifica uma tendência para a propagação dos erros nas decisões do igualizador, especialmente na vizinhança das extremidades do *burst*; note-se, aliás, que as características do modo de transmissão ATM, bem como o débito variável de muitos serviços, são dificilmente compatíveis com um *interleaving* entre *bursts* [14].
- O decodificador interno opera sobre decisões brandas quanto aos símbolos de modulação, com um algoritmo de Viterbi modificado, de acordo com as ideias de [9]; este decodificador é capaz de fornecer ao decodificador externo uma informação implícita sobre o “estado do canal”, sob a forma de ausências de decisão, i.e., rasuras (*erasures*) relativamente a bits com elevada probabilidade de descodificação errónea (na secção 3.2.1 são fornecidos detalhes sobre este processo).
- Não é implementada a correcção dos erros e rasuras pelo decodificador externo para além da capacidade correctora inerente à respectiva distância de Hamming mínima (na secção 3.3 são fornecidos os detalhes correspondentes).

A aplicação da estratégia de controlo de erros é feita de uma forma flexível, tendo em conta as características e requisitos dos serviços. Pressupõe-se o estabelecimento prévio de dois tipos de “limiares” de operação:

- Um limiar interno ( $L$ ) que serve para controlar a produção de rasuras para uso do decodificador externo [9].
- Dois limiares externos ( $L_1$  e  $L_2$ ) que servem para controlar as transmissões dos *bursts* adicionais necessários para concluir a descodificação do conteúdo de cada *burst standard*.

É de salientar que também são utilizadas transmissões adicionais quando o decodificador externo encontra padrões de erros não corrigíveis, de acordo com o terceiro pressuposto atrás enunciado.

Como dissemos atrás, o decodificador interno emprega uma versão modificada do algoritmo de Viterbi. Esta fornece não só a sequência decodificada (com máxima verosimilhança) como também uma informação sobre a fiabilidade das decisões quanto aos diversos bits dessa sequência. Mais concretamente, os bits que são vistos como “provavelmente errados” são substituídos por rasuras; assim, a saída do decodificador interno consiste num misto de bits efectivos e bits rasurados. Os sextetos de bits contendo pelo menos um bit errado são encarados pelo decodificador externo como “símbolos RS” rasurados.

O número de símbolos RS rasurados, por cada bloco de código (42,36), é comparado com os dois limiares externos, “superior” e “inferior” ( $L_2$  e  $L_1$  respectivamente, com  $L_2 > L_1$ ), apropriadamente seleccionados. O número de rasuras RS dá-nos uma informação importante sobre o “estado do canal”; comparando esse número com  $L_1$  e  $L_2$ , podemos classificar implicitamente o canal como “bom”, “relativamente mau” ou “muito mau”, tendo em atenção a qualidade de serviço requerida. Certamente, tem de ser feita uma escolha de compromisso realista para o limiar interno: se  $L$  for muito alto, um número muito elevado de bits correctos serão substituídos por rasuras (i.e., a probabilidade de “falsos alarmes” torna-se elevada), o que significa uma avaliação muito pessimista da qualidade da ligação; se  $L$  for muito baixo, é inevitável uma avaliação optimista da qualidade da ligação e uma percentagem elevada de bits errados não será substituída por rasuras (i.e., a probabilidade de acontecimentos de erro não detectados pode tornar-se inaceitavelmente alta).

O protocolo de controlo de erros ARQ/FEC, ilustrado no fluxograma da figura 3.2, está patente na seguinte sequência de operações:

1. Transmitir o *burst standard* (672 bits de informação codificada, mais bits de treino e caudas), retendo o conteúdo útil do *burst* médio complementar, para o caso de vir a ser necessário.
2. Usar o algoritmo de Viterbi modificado, com decisão branda e limiar  $L$ .

3. Classificar o “estado do canal”, por contagem dos sextetos (símbolos RS) rasurados no primeiro e no segundo blocos de código RS(42,36),  $\rho_1$  e  $\rho_2$ , respectivamente:
  - Se  $\rho_1 > L_2$  ou  $\rho_2 > L_2$  (isto é, o canal encontra-se em “muito mau” estado), então rejeitar o *burst* recebido, suscitando a execução do passo 1, etc.
  - Se  $\rho_1 \leq L_1$  e  $\rho_2 \leq L_1$ , tentar realizar a descodificação RS; se a descodificação é feita com sucesso em ambos os blocos RS(42,36), é enviada uma “confirmação positiva” (ACK: positive acknowledgement), caso contrário é enviada a indicação de que a informação não foi bem recebida (NAK: negative acknowledgement), solicitando expressamente a execução do passo 4, etc.
  - Se o par  $(\rho_1, \rho_2)$  não cumprir as duas condições anteriores, enviar um NAK ao transmissor, para este executar o passo 4, etc.
4. Transmitir o *burst* médio, isto é, 288 bits de redundância adicional, mais bits de treino e caudas (Uma vez que o canal não foi considerado “muito mau”, o *burst standard* inicialmente recebido não é de rejeitar).
5. Utilizar o algoritmo de Viterbi, com decisão branda e o mesmo limiar  $L$ , de novo para efectuar a descodificação interna e fornecer informação sobre a respectiva fiabilidade ao descodificador externo.
6. Realizar a descodificação RS(60,36); se a descodificação for bem sucedida em ambos os blocos, enviar um ACK ao transmissor; se não, enviar um NAK solicitando a execução do passo 4, etc, se esta for a primeira falha na descodificação com o *burst* médio, e, se já o não for, executar o passo 1, etc.

O esquema adaptativo de controlo de erros aqui proposto combina capacidades de correcção e detecção de erros, sob uma avaliação implícita do estado do canal, umas vezes rejeitando e outras tirando partido do *burst* recebido antes e que não se mostrou capaz de garantir uma descodificação com sucesso. Este esquema selecciona as transmissões adicionais de forma a adaptar a redundância do código ao estado do canal e à qualidade de serviço requerida, através da escolha apropriada do limiar interno ( $L$ )

e dos limiares externos ( $L_1$ ,  $L_2$ ). Note-se que estes limiares, em princípio previamente fixados, também podem ser variáveis durante a transmissão, de acordo com os requisitos canal/serviço. Espera-se que esta estratégia de controlo de erros possa ser compatibilizada sem dificuldade com outros aspectos do interface rádio (nomeadamente controlo de potência e controlo de acesso).

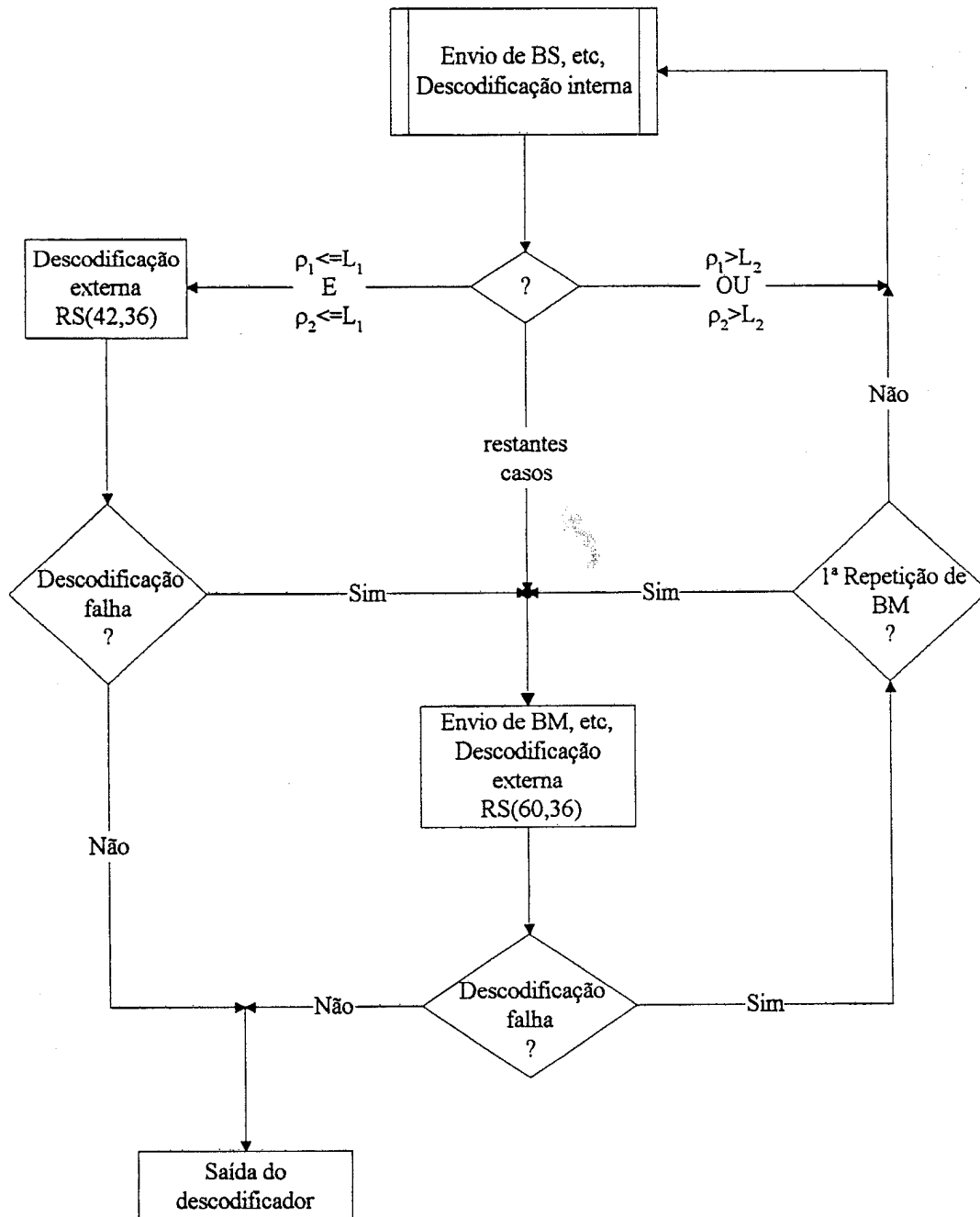


Figura 3. 2: Fluxograma do esquema de controlo de erros.

## 3.2 Códigos interno e externo

### 3.2.1 Código interno

#### 3.2.1.1 Codificação

O código interno é um código convolucional binário de “rendimento” (razão) 3/4 obtido por perfuração (*puncturing*) de um código de rendimento 1/2 [15, 16]. O codificador básico, representado na figura 3.3, pode ser visto como uma máquina de estados finita:  $2^4=16$  estados, no nosso caso, devido aos quatro elementos de atraso presentes no respectivo registador de deslocamento (*shift register*). De acordo com a figura,

$$c_{2i-1} = b_i \oplus b_{i-1} \oplus b_{i-2} \oplus b_{i-3} \oplus b_{i-4}$$
$$c_{2i} = b_i \oplus b_{i-2} \oplus b_{i-4}$$

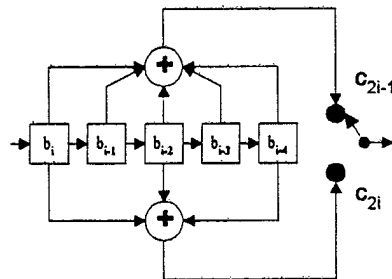


Figura 3. 3: Codificador convolucional.

A perfuração adoptada, que permite obter o código de rendimento 3/4, é realizada como o *trellis* da figura 3.4 indica, por supressão regular, assinalada pelo símbolo X, de alguns dos bits gerados pelo codificador (supressão de dois em cada seis). Como sucede com qualquer código convolucional, a sequência de código corresponde a um percurso no *trellis*; este é completamente determinado pelo estado inicial (por exemplo 0000) e pela sequência binária que é aplicada na entrada do codificador.

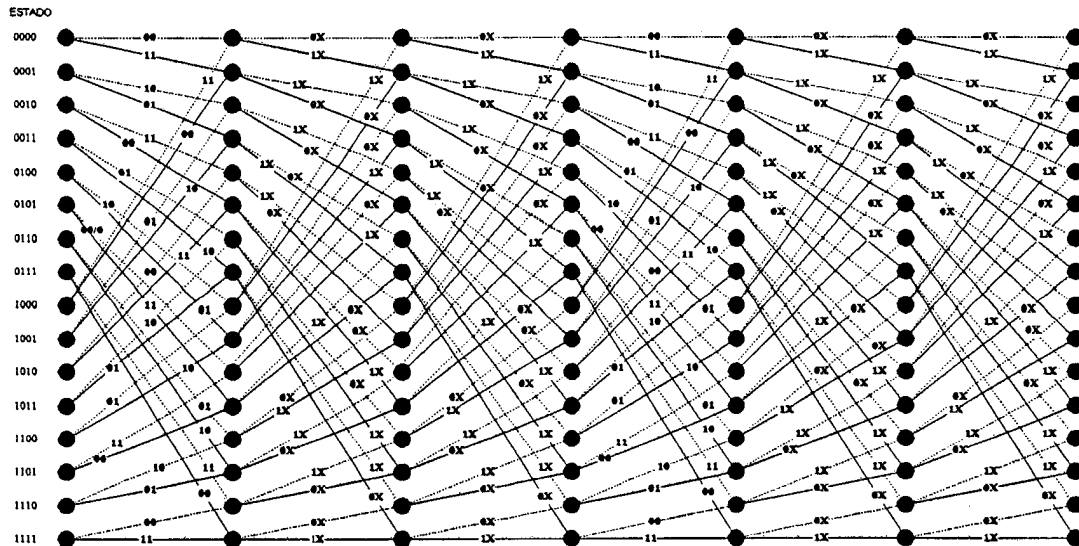


Figura 3. 4: Trellis do código convolucional perfurado.

É sabido que a distância de Hamming “livre” (*free Hamming distance*),  $d_f$ , dum código convolucional traduz as capacidades de correcção de erros do código, quando o decodificador opera sobre decisões rígidas quanto aos símbolos de modulação. Trata-se de uma distância mínima, que, no código adoptado, é igual a quatro: este facto é ilustrado pelos dois percursos assinalados na figura 3.5, correspondentes a seqüências de código que só divergem num intervalo abrangendo seis blocos.

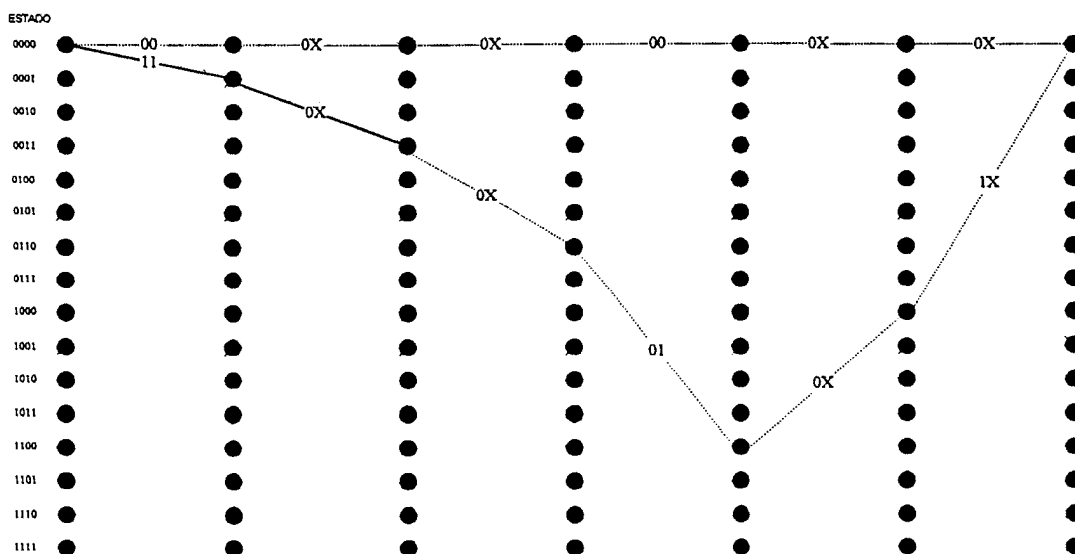


Figura 3. 5: Par de seqüências de código distando  $d_f=4$ .

### 3.2.1.2 Descodificação

O descodificador proposto emprega uma versão modificada, descrita em [9], do bem conhecido algoritmo de Viterbi, inicialmente proposto em [17]. O algoritmo de Viterbi é, desde então, muito utilizado na prática, tanto para fins de descodificação de códigos convolucionais como para outras finalidades. Este algoritmo realiza essencialmente uma descodificação de máxima verosimilhança; no entanto, a carga computacional é relativamente reduzida, pois o algoritmo tira partido da estrutura específica do *trellis* do código, não sendo a complexidade do descodificador função do número de símbolos da sequência a descodificar. Uma descodificação por comparação exaustiva, tendo em conta todas as sequências possíveis, teria uma complexidade exponencialmente crescente com o comprimento da sequência codificada. A aplicação do algoritmo de Viterbi exige o cálculo de “métricas” associadas aos ramos do *trellis*; a cada novo bloco recebido, a “métrica” de um ramo constitui uma medida da similaridade entre o sinal recebido e o sinal correspondente a esse ramo. A cada novo bloco, o algoritmo escolhe um de entre os vários percursos que, no *trellis*, conduzem a cada um dos diversos estados, eliminando os restantes: trata-se do chamado “sobrevivente”. A escolha traduz um critério de máxima verosimilhança, baseando-se na similaridade entre o sinal recebido e os sinais correspondentes aos percursos candidatos, até esse instante; para cada percurso, a similaridade (maior ou menor) é expressa pela respectiva “métrica acumulada” ao longo do mesmo, que consiste no somatório das “métricas” associadas aos ramos que o compõem. A rejeição de vários percursos (todos menos um, por cada estado), a cada ciclo do algoritmo de Viterbi, obviamente contribui para reduzir a complexidade computacional. Quando o código convolucional é perfurado (como acontece com o código apresentado na secção 3.2.1.1), os bits codificados de cada bloco podem não ser todos efectivamente transmitidos; contudo, é como se o fossem, para efeitos de “sincronização” dos procedimentos de descodificação, de acordo com o algoritmo de Viterbi, embora a respectiva contribuição para as métricas seja nula.

O modo de proceder para obter as métricas dos ramos, no quadro duma decisão branda, é o seguinte: obtida(s) a(s) amostra(s) que, na entrada do bloco decisor do

DFE, corresponde(m) ao bloco recebido (uma ou duas, consoante há ou não perfuração, veja-se o *trellis* da figura 3.4), efectua-se a soma algébrica das mesmas, com o peso +1 ou -1 consoante há um “1” ou um “0”, respectivamente, no ramo em questão.

O algoritmo de descodificação de códigos convolucionais proposto em [9] pode ser visto como uma modificação do algoritmo de Viterbi, para aplicações práticas em que aqueles constituem “códigos internos” num sistema de códigos concatenados. A citada modificação preserva todos os procedimentos inerentes ao algoritmo de Viterbi, permitindo obter a sequência “com máxima verosimilhança” na saída do descodificador; a modificação consiste na realização de operações adicionais que permitem informar o descodificador externo quanto à fiabilidade das sucessivas decisões do descodificador interno. Os bits descodificados (de acordo com os procedimentos em tudo idênticos aos do algoritmo de Viterbi) sobre os quais recaia a “suspeita” de estarem errados são substituídos por rasuras, para efeitos de descodificação externa; por outras palavras, a modificação consiste em “apagar” os bits descodificados que, de acordo com um certo critério, podem ser considerados como “provavelmente errados”.

Vejam os em seguida a ideia que está na base deste processo de decodificação:

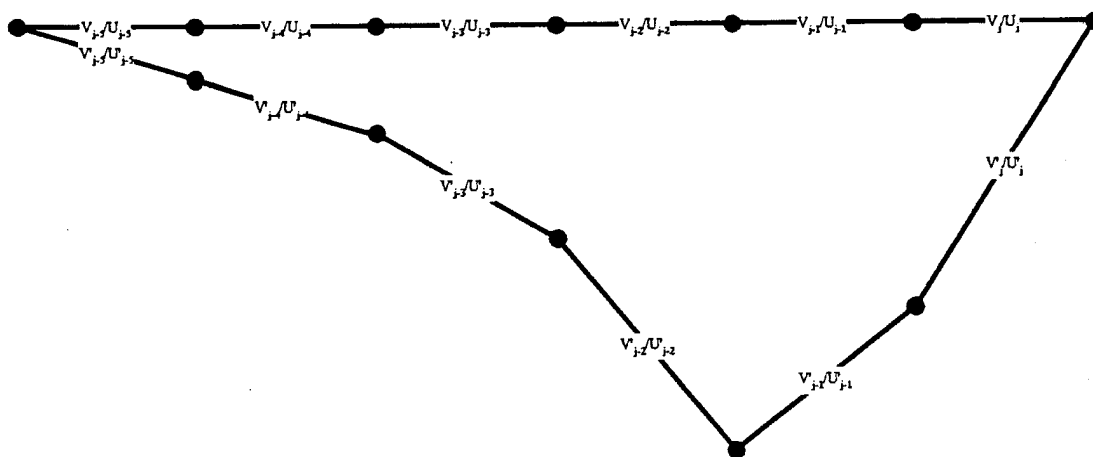


Figura 3. 6: Ilustração de um “acontecimento de erro” abarcando seis ramos.

Supondo que houve, na descodificação, um primeiro acontecimento de erro num nível  $j$  arbitrário, o ramo correcto, assinalado por  $V_j$  (bloco de código) ou  $U_j$  (bloco de informação) é eliminado em benefício do ramo incorrecto ( $V'_j$  ou  $U'_j$ ), o mesmo sucedendo a alguns ramos precedentes.

Se designarmos as métricas acumuladas por  $\lambda_j$  e  $\lambda'_j$ , respectivamente, pode dizer-se que o erro resultou de ser mais verosímil o percurso errado do que o percurso correcto, isto é,  $\lambda'_j > \lambda_j$ , ao contrário do que sucederia obrigatoriamente se a descodificação fosse perfeita (na ausência de ruído, etc.); as métricas acumuladas  $\lambda_j$  e  $\lambda'_j$  representam “medidas de verosimilhança” dos percursos que terminam nos referidos ramos  $V_j(U_j)$  e  $V'_j(U'_j)$ , respectivamente. A modificação proposta em [9] consiste em determinar, não só o percurso de maior verosimilhança que culmina em cada estado, mas também o “segundo classificado”: se a diferença entre as métricas acumuladas estiver abaixo de um certo limiar  $L$ , todos os bits de informação que diferirem num e noutro dos dois percursos mais verosímeis são rasurados; caso contrário, isso não acontece, sendo todos os bits tidos como fiáveis. No exemplo da figura 3.6 (em que admitimos ser  $\lambda'_j > \lambda_j$ ), haveria que comparar  $\lambda'_j - \lambda_j$  com  $L$ , se fossem  $\lambda'_j$  e  $\lambda_j$  as duas maiores métricas. Sendo  $\lambda'_j - \lambda_j < L$ , os bits diferentes no par de blocos  $U_{j-5}$  e  $U'_{j-5}$  seriam apagados, o mesmo se podendo dizer dos bits diferentes nos pares de blocos  $(U_{j-4}, U'_{j-4})$ ,  $(U_{j-3}, U'_{j-3})$ ,  $(U_{j-2}, U'_{j-2})$  e  $(U_{j-1}, U'_{j-1})$ . Note-se que, no caso do código convolucional perfurado aqui proposto, é reduzido o incremento de complexidade computacional inerente à modificação do algoritmo de Viterbi: como o *trellis* da figura 3.4 mostra, só há dois percursos candidatos, para cada estado, pelo que só há que comparar esses dois para determinar o “sobrevivente” e o “segundo classificado”.

Obviamente, as rasuras tendem a aumentar com o aumento de  $L$ ; pelo contrário, se  $L=0$  estaríamos em presença do algoritmo de Viterbi convencional, sem produção de rasuras. Um valor muito baixo de  $L$  não possibilita a identificação de muitos acontecimentos de erro; inversamente, um valor muito elevado de  $L$  leva a um excesso de rasuras, podendo muitas delas cobrir decisões correctas do descodificador. Na prática, há que adoptar soluções de compromisso, como veremos no capítulo 4, pois tanto as “falhas de detecção” de acontecimentos de erro como os “falsos alarmes” prejudicam o desempenho quando excessivos.

### 3.2.2 Código externo

Nesta tese é dado um relevo especial ao código de controlo de erros externo. Como dissemos anteriormente, este deriva dum código Reed-Solomon (RS) construído sobre o campo finito  $GF(2^6)$ ; isto é, cada “símbolo RS” é formado por um sexteto de símbolos binários. Os códigos RS são códigos lineares que podem ser vistos como constituindo uma subclasse no âmbito da classe, mais geral, de códigos cíclicos BCH (Bose-Chaudhuri-Hocquenghem) [10,18]. Os códigos RS têm especial interesse prático como códigos externos num arranjo de códigos concatenados: a descodificação do código interno, binário, produz por vezes rajadas de erros; cada uma destas pode abarcar um número muito pequeno de símbolos, não-binários, do código externo (frequentemente um só símbolo). No nosso caso, os acontecimentos de erro mais frequentes na descodificação interna correspondem à troca da sequência de código correcta por uma que dela dista o mínimo, isto é,  $d_1=4$  (ver figuras 3.4 e 3.5). As sequências de informação correspondentes diferem apenas em dois bits consecutivos, o primeiro e o segundo dos seis que o acontecimento de erro abarca. Dada a maneira como os sextetos de bits são organizados em “símbolos RS”, é evidente que os dois erros consecutivos atrás referidos se localizarão na parêlha (1º bit, 2º bit) ou na parêlha (4º bit, 5º bit) de um certo símbolo RS. Isto significa que o acontecimento de erro mais frequente na descodificação interna envolve apenas um símbolo RS; se detectássemos este acontecimento de erro graças a um limiar interno suficientemente elevado, apareceriam rasuras numa ou noutra das parêlhas atrás referidas, pelo que, por motivos idênticos, apenas um símbolo RS seria rasurado. Evidentemente que, na prática, se registam outros acontecimentos de erro, ainda que com menor frequência; embora possam envolver um certo número de símbolos RS, pode dizer-se que esse número é, em média, claramente inferior ao número de símbolos binários envolvidos, devido à tendência para o agrupamento destes.

Os códigos RS construídos sobre  $GF(2^m)$  são códigos  $(N,K)$  em que cada símbolo RS é formado por  $m$  bits,  $N=2^m-1$ ,  $N-K$  é par e a distância de Hamming mínima,  $d_{min}$ , verifica o “limite de Singleton”, isto é,  $d_{min}=N-K+1$  [10]. Isto significa que, quando usados em sistema FEC convencional, garantem a correcção de  $t$  erros se  $2t=N-K$ . Um código “RS encurtado”  $(N-b,K-b)$  tem uma capacidade de controlo de erros pelo

menos igual à do código RS(N,K) de que deriva. No nosso caso, parte-se dum código RS(63,39), resultando deste o código encurtado RS(60,36) com a mesma distância de Hamming  $d_{\min}=25$ . Quando se pretende a descodificação de blocos com  $\rho$  rasuras, é sabido que está garantida a correcção de  $t'$  erros se  $2t'+\rho+1 \leq d_{\min}$ . Para o código RS(60,36) que aqui recomendamos, é válida a tabela seguinte:

**Tabela 3. 1**

Rasuras	Erros
0	12
1,2	11
3,4	10
5,6	9
7,8	8
9,10	7
11,12	6
13,14	5
15,16	4
17,18	3
19,20	2
21,22	1
23,24	0

Como assinalámos anteriormente, a construção de cada *burst standard* envolve dois blocos de um código RS(42,36) obtido por perfuração do código encurtado RS(60,36). Este código apresenta  $d_{\min}=42-36+1=7$ , correspondendo-lhe, por conseguinte, a tabela 3.2:

**Tabela 3. 2**

Rasuras	Erros
0	3
1,2	2
3,4	1
5,6	0

A terminar esta secção, mostra-se como se constrói um campo finito de Galois  $GF(2^m)$ , como extensão de  $GF(2)$ , como se definem os símbolos  $2^m$ -ários e como se processa a codificação externa, recorrendo a um adequado “polinómio gerador” dum

código RS( $2^m-1, 2^m-1-2t$ ) (no nosso caso,  $m=6$  e  $t=12$ ). A secção 3.3 aborda, detalhadamente, o problema da descodificação externa no âmbito da estratégia de controlo de erros proposta. A abordagem aqui usada segue de perto [10,19].

### 3.2.2.1 Construção de $GF(2^6)$ e definição de símbolos RS $2^6$ -ários

A construção de  $GF(2^m)$  como extensão de  $GF(2)$  é realizada “módulo  $p(x)$ ”, em que  $p(x)$ , de grau  $m$ , é um “polinómio primitivo” definido sobre  $GF(2)$ . A cada elemento de  $GF(2^m)$  corresponde um polinómio definido sobre  $GF(2)$ , com grau inferior a  $m$ . Num código RS construído sobre  $GF(2^m)$ , cada símbolo  $2^m$ -ário corresponde a um elemento de  $GF(2^m)$ ; os  $m$  bits que o compõem são os  $m$  coeficientes binários do polinómio (de grau inferior a  $m$ ) respectivo. Sendo  $p(x)$  um polinómio primitivo, o elemento de  $GF(2^m)$  correspondente a  $x$  -e que designaremos por  $\alpha$ - é um “elemento primitivo”: por conseguinte, todo e qualquer elemento de  $GF(2^m)$ , com a excepção de 0, pode ser expresso sob a forma duma potência de  $\alpha$ . Mais precisamente, pode dizer-se que os  $2^m$  elementos de  $GF(2^m)$  são da forma seguinte:  $0, \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{N-1}$  ( $N=2^m-1$ ). Potências de base  $\alpha$  com outros expoentes conduzem sempre a elementos de  $GF(2^m)$ , pois  $\alpha^n = \alpha^{n \bmod N}$ . O polinómio correspondente a cada  $\alpha^n$  é  $x^{n \bmod p(x)}$  (leia-se: o resto da divisão de  $x^n$  por  $p(x)$ ). A tabela 3.3 refere-se ao nosso caso particular, isto é,  $m=6$ , quando é usado o polinómio primitivo  $p(x)=x^6+x+1$ : ela define os  $2^6-1=63$  elementos não nulos de  $GF(2^6)$ , quer sob a forma de potências de base  $\alpha$ , quer sob a forma de sextetos de bits; o polinómio associado a cada elemento de  $GF(2^6)$  está implícito no sexteto de bits indicado, com a ordem crescente dos graus em consonância com a leitura do sexteto da esquerda para a direita (por exemplo  $\alpha^{11}$  corresponde a  $x^5+x+1$ ). Para construirmos a tabela 3.3 podemos tirar partido da representação dos elementos não nulos de  $GF(2^m)$  como potências de base  $\alpha$ , efectuando as multiplicações requeridas:  $\alpha^n \cdot \alpha^p = \alpha^{n+p} = \alpha^{(n+p) \bmod N}$ .

Por exemplo (no nosso caso):

$$\alpha^6 = x^6 \bmod (x^6 + x + 1) = 1 + x \leftrightarrow [110000]$$

$$\alpha^7 = \alpha \cdot \alpha^6 = [x(x+1)] \bmod (x^6 + x + 1) = x + x^2 \leftrightarrow [011000], \text{ etc.}$$

**Tabela 3. 3**

$\alpha^n$	$x^0x^1x^2x^3x^4x^5$	$\alpha^n$	$x^0x^1x^2x^3x^4x^5$	$\alpha^n$	$x^0x^1x^2x^3x^4x^5$	$\alpha^n$	$x^0x^1x^2x^3x^4x^5$
$\alpha^0$	100000	$\alpha^{16}$	110010	$\alpha^{32}$	100100	$\alpha^{48}$	101100
$\alpha^1$	010000	$\alpha^{17}$	011001	$\alpha^{33}$	010010	$\alpha^{49}$	010110
$\alpha^2$	001000	$\alpha^{18}$	111100	$\alpha^{34}$	001001	$\alpha^{50}$	001011
$\alpha^3$	000100	$\alpha^{19}$	011110	$\alpha^{35}$	110100	$\alpha^{51}$	110101
$\alpha^4$	000010	$\alpha^{20}$	001111	$\alpha^{36}$	011010	$\alpha^{52}$	101010
$\alpha^5$	000001	$\alpha^{21}$	110111	$\alpha^{37}$	001101	$\alpha^{53}$	010101
$\alpha^6$	110000	$\alpha^{22}$	101011	$\alpha^{38}$	110110	$\alpha^{54}$	111010
$\alpha^7$	011000	$\alpha^{23}$	100101	$\alpha^{39}$	011011	$\alpha^{55}$	011101
$\alpha^8$	001100	$\alpha^{24}$	100010	$\alpha^{40}$	111101	$\alpha^{56}$	111110
$\alpha^9$	000110	$\alpha^{25}$	010001	$\alpha^{41}$	101110	$\alpha^{57}$	011111
$\alpha^{10}$	000011	$\alpha^{26}$	111000	$\alpha^{42}$	010111	$\alpha^{58}$	111111
$\alpha^{11}$	110001	$\alpha^{27}$	011100	$\alpha^{43}$	111011	$\alpha^{59}$	101111
$\alpha^{12}$	101000	$\alpha^{28}$	001110	$\alpha^{44}$	101101	$\alpha^{60}$	100111
$\alpha^{13}$	010100	$\alpha^{29}$	000111	$\alpha^{45}$	100110	$\alpha^{61}$	100011
$\alpha^{14}$	001010	$\alpha^{30}$	110011	$\alpha^{46}$	010011	$\alpha^{62}$	100001
$\alpha^{15}$	000101	$\alpha^{31}$	101001	$\alpha^{47}$	111001	0	000000

Para adicionar dois elementos de  $GF(2^m)$  pode usar-se a respectiva representação binária (ou os polinómios correspondentes, definidos sobre  $GF(2)$ ). Por exemplo:

$$\alpha^{56} + \alpha^{15} = (x^4 + x^3 + x^2 + x + 1) + (x^5 + x^3) = x^5 + x^4 + x^2 + x + 1 = \alpha^{43} \leftrightarrow [111011].$$

A subtração de dois elementos de  $GF(2^m)$  conduz ao mesmo resultado que a adição.

Um processo expedito para adicionar elementos de  $GF(2^m)$  recorre aos chamados “logaritmos de Zech”,  $L(Z)$ , assim definidos [18]:  $\alpha^{L(Z)} = \alpha^Z + 1$ . Então

$$\alpha^n + \alpha^m = \alpha^m (\alpha^{n-m} + 1) = \alpha^{m+L(n-m)} = \alpha^{[m+L(n-m)] \bmod (N)}$$

Aplicando esta ideia ao nosso caso, podemos construir a tabela 3.4 de logaritmos de Zech (note-se que  $\alpha^{L(1)} = \alpha^1 + 1 = x + 1 = \alpha^6$ ,  $\alpha^{L(2)} = \alpha^2 + 1 = x^2 + 1 = \alpha^{12}$ , etc.).

Tabela 3. 4

Z	L(Z)	Z	L(Z)	Z	L(Z)
		21	42	42	21
1	6	22	50	43	39
2	12	23	15	44	37
3	32	24	4	45	9
4	24	25	11	46	30
5	62	26	7	47	41
6	1	27	18	48	8
7	26	28	41	49	38
8	48	29	60	50	22
9	45	30	46	51	53
10	61	31	34	52	14
11	25	32	3	53	51
12	2	33	16	54	36
13	35	34	31	55	40
14	52	35	13	56	19
15	23	36	54	57	58
16	33	37	44	58	57
17	47	38	49	59	20
18	27	39	43	60	29
19	56	40	55	61	10
20	59	41	28	62	5

Consultando a tabela 3.4 pode obter-se  $\alpha^{56} + \alpha^{15} = \alpha^{15+L(41)} = \alpha^{15} + \alpha^{L(41)} = \alpha^{15+28} = \alpha^{43}$ , etc.

### 3.2.2.2 Codificação externa

O código externo deriva dum código RS construído sobre  $GF(2^6)$ . Este é um código cíclico  $(2^m-1, 2^m-1-2t)$ , cujo polinómio gerador, definido sobre  $GF(2^m)$  (no nosso caso  $m=6$ ), pode ser escrito na forma

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3) \dots (x-\alpha^{2t}) \tag{3.1}$$

Tendo escolhido um código de base  $(63,39)$ , isto significa que  $t=12$ , pelo que

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3) \dots (x-\alpha^{24}) = \alpha^{63}x^{24} + \alpha^{62}x^{23} + \alpha^4x^{22} + \alpha^{25}x^{21} + \alpha^{47}x^{20} + \alpha^{49}x^{19} + \alpha^{47}x^{18} + \alpha^{55}x^{17} + \alpha^{62}x^{16} + \alpha^{59}x^{15} + \alpha^{31}x^{14} + \alpha^6x^{13} + \alpha^{51}x^{12} + \alpha^{31}x^{11} + \alpha^{18}x^{10} + \alpha^8x^9 + \alpha^{36}x^8 + \alpha^{54}x^7 + \alpha^8x^6 + \alpha^{35}x^5 + \alpha^{58}x^4 + \alpha^{61}x^3 + \alpha^2x^2 + \alpha^{22}x + \alpha^{48} \tag{3.2}$$

O código RS(63,39) proposto é um código sistemático, isto é, cada bloco de código é formado por dois sub-blocos, um deles constituído só pelos 39 símbolos de informação correspondentes, e o outro constituído só pelos  $63-39=24$  símbolos redundantes (símbolos de paridade). Utilizando representação polinomial para o bloco de informação,

$$i(x)=i_0+i_1x+\dots+i_{38}x^{38} \quad (3.3)$$

em que os coeficientes  $i_0, i_1, \dots, i_{38}$  são elementos de  $GF(2^6)$ , o polinómio associado ao bloco de símbolos redundantes deverá ser

$$r(x)=[x^{24}i(x)]\text{mod}(g(x))=r_0+r_1x+\dots+r_{23}x^{23} \quad (3.4)$$

com  $g(x)$  e  $i(x)$  dados por (3.2) e (3.3), respectivamente.

Estando associado a cada bloco de código  $[c_0 c_1 \dots c_{62}]$  também um polinómio, adoptou-se

$$c(x)=r(x)+x^{N-K}i(x)=r(x)+x^{24}i(x)=c_0+c_1x+\dots+c_{62}x^{62} \quad (3.5)$$

em que  $c_j=r_j$  para  $j=0,1,\dots,23$  e  $c_j=i_{j-24}$  para  $j=24,25,\dots,62$ . Note-se que também era legítimo colocar os sub-blocos de informação e paridade de forma inversa, isto é,

$$c(x)=i(x)+x^Kr(x)=i(x)+x^{39}r(x)=c_0+c_1x+\dots+c_{62}x^{62} \quad (3.6)$$

com  $c_j=i_j$  para  $j=0,1,\dots,38$  e  $c_j=r_{j-39}$  para  $j=39,40,\dots,62$ .

O código externo recomendado constitui uma versão encurtada do código RS(63,39). Pretendendo-se um código (60,36), pode usar-se um codificador RS(63,39) com  $i_{36}=i_{37}=i_{38}=0$ . Isto implica necessariamente  $c_{60}=c_{61}=c_{62}=0$ , não sendo estes três símbolos efectivamente transmitidos. Os blocos (42,36) usados para efeitos de construção do *burst standard* excluem  $60-42=18$  símbolos de paridade: são portanto blocos  $[c_{18} c_{19} \dots c_{59}]$ . Os blocos complementares usados na construção

dos *bursts* médios são constituídos pelos símbolos inicialmente retidos, isto é, são blocos  $[c_0 c_1 \dots c_{17}]$ .

### 3.3 Descodificação externa

O problema da descodificação externa é tratado nesta secção, seguindo de perto a abordagem de Blahut em [10] e [19] relativamente a códigos Reed-Solomon. Quer o que designamos por “descodificação externa RS(42,36)” quer o que designamos por “descodificação externa RS(60,36)” (ver figura 3.2) é realizado pelo mesmo descodificador: este é desenhado para corrigir erros e rasuras no âmbito dum código RS construído sobre  $GF(2^6)$ , com  $N=2^6-1=63$  e  $t=12$ , isto é,  $K=N-2t=39$ . O descodificador pode ainda detectar “erros não corrigíveis”, o que corresponde às “falhas da descodificação” assinaladas na figura 3.2 (não confundir com os “erros na descodificação” que por vezes surgem quando a correcção é consumada). Para efeitos de descodificação externa RS(60,36), acrescentam-se três zeros ao bloco recebido  $[v_0 v_1 \dots v_{59}]$ , de modo a que o descodificador RS(63,39) efectue a descodificação do bloco  $[v_0 v_1 \dots v_{59} 0 0 0]$  (trata-se de uma operação complementar do encurtamento realizado na emissão); alguns dos  $v_i$ 's representam símbolos RS, outros representam rasuras cuja colocação é controlada pelo descodificador interno, através do limiar respectivo. Para efeitos de descodificação externa RS(42,36), não só se acrescentam três zeros no fim do bloco recebido  $[v_{18} v_{19} \dots v_{59}]$ , mas também 18 rasuras no seu início, em correspondência com os 18 símbolos de paridade inicialmente retidos; ou seja, no bloco  $[v_0 v_1 \dots v_{59} 0 0 0]$  a descodificar há sempre pelo menos 18  $v_i$ 's rasurados ( $i=0,1,\dots,17$ ).

Nesta secção descreve-se um algoritmo eficiente para descodificação de códigos RS  $(2^m-1, 2^m-1-2t)$ , construídos sobre  $GF(2^m)$  (é este o caso do código (63,39) que temos vindo a citar). No anexo A são dados alguns exemplos simples de aplicação deste algoritmo a um código RS desta classe com  $m=3$  e  $t=2$ .

### 3.3.1 Introdução

Seja  $c(x)$  o polinómio genérico associado às palavras do código RS( $2^m-1, 2^m-1-2t$ ), definido sobre GF( $2^m$ ) e com polinómio gerador  $g(x)$  dado por (3.1). Como  $c(x)$  é divisível por  $g(x)$  pode escrever-se

$$c(x)=g(x)q(x) \quad (3.7)$$

pelo que

$$c(\alpha^j)=g(\alpha^j)q(\alpha^j)=0, \quad j=1,2,\dots,2t \quad (3.8)$$

pois  $\alpha, \alpha^2, \dots, \alpha^{2t}$  são zeros de  $g(x)$  (ver (3.1)).

Sendo recebido o polinómio

$$v(x)=c(x)+e(x) \quad (3.9)$$

em que  $c(x)$  corresponde à palavra de código transmitida e  $e(x)$  é o “polinómio de erro” (todos estes polinómios de grau não superior a  $N-1=2^m-2$ ), pode escrever-se

$$v(\alpha^j)=e(\alpha^j), \quad j=1, 2, \dots, 2t \quad (3.10)$$

atendendo a (3.8).

Como é sabido, o cálculo do “vector síndrome” da palavra recebida pode desempenhar um papel central no processo de descodificação. O polinómio correspondente, de grau inferior a  $N-K=2t$ , é

$$s(x)=v(x) \bmod (g(x)) \quad (3.11)$$

Uma vez que é possível escrever

$$v(x) = g(x)q_v(x) + s(x) \quad (3.12)$$

torna-se evidente que

$$s(\alpha^j) = v(\alpha^j), \quad j = 1, 2, \dots, 2t \quad (3.13)$$

por ser  $g(\alpha) = g(\alpha^2) = \dots = g(\alpha^{2t}) = 0$

A essência do processo de decodificação com o síndrome consiste em obter uma estimativa do polinómio de erro com base no síndrome  $s(x)$  calculado. Obtida a estimativa  $\hat{e}(x)$ , podemos calcular  $\hat{c}(x) = v(x) - \hat{e}(x)$ ; obviamente,  $\hat{c}(x) = c(x)$  se e só se  $\hat{e}(x) = e(x)$ .

### 3.3.2 Descrição do código RS usando transformadas de Fourier discretas

Seja  $\underline{v} = [v_0 \ v_1, \dots, v_{N-1}]$ , com  $N = 2^m - 1$ , um vector construído sobre  $GF(2^m)$ . A “transformada de Fourier discreta de  $\underline{v}$ ” (ou “espectro de  $\underline{v}$ ”) é definida como o vector  $\underline{V} = [V_0 \ V_1, \dots, V_{N-1}]$ , também construído sobre  $GF(2^m)$ , em que

$$V_j = \sum_{i=0}^{N-1} \alpha^{i \cdot j} v_i, \quad j = 0, 1, \dots, N-1 \quad (3.14)$$

A relação (3.14) é formalmente análoga à que define a bem conhecida transformada Fourier discreta (DFT), no campo complexo:

$$P_k = \sum_{n=0}^{N-1} \omega^{n \cdot k} p_n, \quad k = 0, 1, \dots, N-1 \quad (3.15)$$

em que  $\omega = e^{j(2\pi/N)}$  (aqui  $j = \sqrt{-1}$ ); pode assim dizer-se que o índice  $i$  em (3.14) designa “tempo” e o índice  $j$  designa “frequência”.

Tal como no campo complexo, é possível definir uma IDFT em  $GF(2^m)$ , ou seja

$$v_i = \frac{1}{N} \sum_{j=0}^{N-1} \alpha^{-i \cdot j} V_j, \quad i = 0, 1, \dots, N-1 \quad (3.16)$$

Note-se que as outras propriedades das transformadas de Fourier são também aqui aplicadas:

- Teorema da convolução - a multiplicação no domínio do tempo corresponde a uma convolução no domínio da frequência

$$e_i = f_i g_i \quad (i = 0, 1, \dots, N-1) \Rightarrow E_j = (F * G)_j = \frac{1}{N} \sum_{k=0}^{N-1} F_{((j-k))} G_k, \quad j = 0, 1, \dots, N-1 \quad (3.17)$$

- Propriedade da translacção - se  $\{v_i\} \leftrightarrow \{V_j\}$  são "pares de Fourier" então também temos os seguintes pares de Fourier:

$$\{\alpha^i v_i\} \leftrightarrow \{V_{((i+1))}\} \text{ e } \{v_{((i-1))}\} \leftrightarrow \{\alpha^j V_j\} \quad (3.18)$$

Atendendo a (3.8), pode então dizer-se que um vector  $\underline{c} = [c_0 \ c_1 \ \dots \ c_{N-1}]$  pertencente a um código RS( $2^m-1, 2^m-1-2t$ ) ( $N=2^m-1$ ) tem necessariamente os  $2t$  zeros espectrais seguintes:

$$C_j = 0, \quad j = 1, 2, \dots, 2t \quad (3.19)$$

pois, sendo

$$c(x) = c_0 + c_1 x + \dots + c_{N-1} x^{N-1}, \quad (3.20)$$

Resulta

$$c(\alpha^j) = \sum_{i=0}^{N-1} \alpha^{i \cdot j} c_i = C_j \quad (3.21)$$

Note-se ainda que

$$c_i = \frac{1}{N} C(\alpha^{-i}) \quad (3.22)$$

em que  $C(x) = C_0 + C_1 x + \dots + C_{N-1} x^{N-1}$ .

O que foi feito para os vectores de código pode ser também feito para qualquer outro vector de  $N=2^m-1$  elementos, construído sobre  $GF(2^m)$ . Neste contexto, a relação (3.10) assume a forma

$$V_j = E_j, \quad j=1,2,\dots,2t \quad (3.23)$$

$$\text{se fizermos } V_j = \sum_{i=0}^{N-1} \alpha^{i \cdot j} v_i \text{ e } E_j = \sum_{i=0}^{N-1} \alpha^{i \cdot j} e_i.$$

É importante notar, tendo em consideração (3.13), que os síndromas do vector  $\underline{v}=[v_0 v_1 \dots v_{N-1}]$  recebido são  $N-K=2t$  elementos de  $GF(2^m)$  dados por

$$S_j = s(\alpha^j) = v(\alpha^j) = V_j = E_j, \quad j=1,2,\dots,2t \quad (3.24)$$

Este bloco de síndromas dá-nos assim uma “janela” através da qual podemos observar  $2t$  dos  $N$  componentes do espectro do vector de erros. O decodificador RS que analizaremos em seguida pode ser visto como um decodificador que opera “no domínio da frequência” tendo por tarefa achar, com base nestes, os  $N-2t$  componentes restantes.

### 3.3.3 Algoritmo de Berlekamp-Massey

Seja  $v(x)=c(x)+e(x)$  o polinómio recebido, admitindo-se que  $c(x)$  pertence ao código, isto é,  $c(\alpha^j)=0$  para  $j=1,2,\dots,2t$ , e que  $e(x)$  é o polinómio de erros. Suponhamos que ocorrem  $h \leq t$  erros; ao iniciar o processo de descodificação o decodificador ignora o valor de  $h$ , bem como a localização dos erros e a sua amplitude. Os  $2t$  síndromas anteriormente referidos (ver (3.24)) podem ser escritos na forma

$$S_j = \sum_{i=0}^{N-1} \alpha^{i \cdot j} e_i, \quad j=1,2,\dots,2t \quad (3.25)$$

mas também na forma

$$S_j = e_{i_1} \alpha^{j i_1} + e_{i_2} \alpha^{j i_2} + \dots + e_{i_h} \alpha^{j i_h}, \quad j = 1, 2, \dots, 2t \quad (3.26)$$

se tivermos em conta um polinómio de erros com  $h$  coeficientes não nulos, isto é, um polinómio  $e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + \dots + e_{i_h} x^{i_h}$  em que os  $i_n$  designam as localizações dos erros e os  $e_{i_n}$  as respectivas amplitudes.

Adoptando as notações  $Y_n = e_{i_n}$  e  $X_n = \alpha^{i_n}$ , para  $n=1, 2, \dots, h$ , podemos escrever o seguinte conjunto de  $2t$  equações:

$$S_j = Y_1 X_1^j + Y_2 X_2^j + \dots + Y_h X_h^j = \sum_{n=1}^h X_n^j Y_n, \quad j = 1, \dots, 2t \quad (3.27)$$

Estas equações não lineares -em que  $X_1, X_2, \dots, X_h$  representam as localizações dos erros e  $Y_1, Y_2, \dots, Y_h$  as respectivas amplitudes- têm uma solução única. Para obtermos essa solução há que considerar o "polinómio de localização dos erros"

$$\Lambda(x) = \Lambda_h x^h + \Lambda_{h-1} x^{h-1} + \dots + \Lambda_1 x + 1 \quad (3.28)$$

assim chamado por ter zeros para  $X_1^{-1}, X_2^{-1}, \dots, X_h^{-1}$ . Isto é,

$$\Lambda(x) = (1 - xX_1)(1 - xX_2) \dots (1 - xX_h). \quad (3.29)$$

Multiplicando ambos os membros de (3.28) por  $Y_n X_n^{j+h}$  e fazendo  $x = X_n^{-1}$  obtém-se

$$Y_n X_n^{j+h} (1 + \Lambda_1 X_n^{-1} + \Lambda_2 X_n^{-2} + \dots + \Lambda_h X_n^{-h}) = 0 \quad (3.30)$$

ou

$$Y_n (X_n^{j+h} + \Lambda_1 X_n^{j+h-1} + \Lambda_2 X_n^{j+h-2} + \dots + \Lambda_h X_n^j) = 0 \quad (3.31)$$

equação esta que é válida para cada  $n \in (1, 2, \dots, h)$  e cada  $j \in (1, 2, \dots, 2t)$ .

Fazendo o somatório destas equações para  $n=1, \dots, h$ , obtém-se, para cada  $j$ ,

$$\sum_{n=1}^h Y_n X_n^{j+h} + \Lambda_1 \sum_{n=1}^h Y_n X_n^{j+h-1} + \dots + \Lambda_h \sum_{n=1}^h Y_n X_n^j = S_{j+h} + \Lambda_1 S_{j+h-1} + \dots + \Lambda_h S_j = 0 \quad (3.32)$$

atendendo a (3.27).

Como  $h \leq t$ , os índices especificam sempre síndromas conhecidos se  $1 \leq j \leq h$ . Chegamos assim ao sistema de equações lineares:

$$S_{j+h} = -\Lambda_1 S_{j+h-1} - \dots - \Lambda_h S_j, \quad j = 1, 2, \dots, h \quad (3.33)$$

ou, o que é equivalente,

$$S_j = \sum_{i=1}^h \Lambda_i S_{j-i}, \quad j = h+1, \dots, 2h \quad (3.34)$$

Uma forma de resolver eficientemente este sistema de equações é proporcionada pelo chamado "algoritmo de Berlekamp-Massey" [10,19,20,21], cujo desenvolvimento pode ser visto como um problema de desenho de circuitos lineares recursivos, baseados em registradores de deslocamento (Ver figura 3.7).

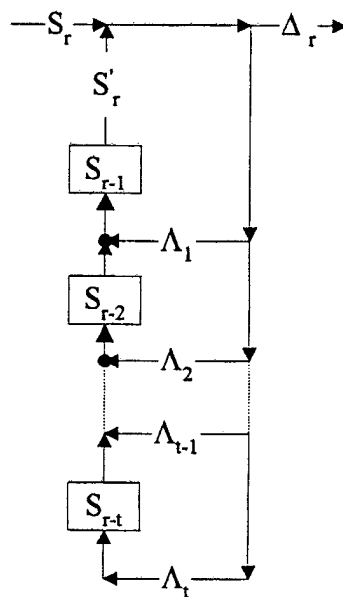


Figura 3. 7: Circuito linear associado ao algoritmo de Berlekamp-Massey.

Este algoritmo consiste em calcular recursivamente, em  $2t$  iterações, os coeficientes do polinómio de localização de erros  $\Lambda(x)$ , cujo grau não pode ser maior que o comprimento dos registadores de deslocamento do circuito da figura 3.7. O problema a resolver transforma-se no da determinação dos parâmetros do circuito capaz de gerar a sequência de síndromas conhecidos. O procedimento adoptado é indutivo: para cada  $r$ , sendo  $r_{\text{inicial}}=1$ , podemos desenhar o registador de deslocamento para gerar os primeiros  $r$  síndromas. O registador de deslocamento  $(L^{(r)}, \Lambda^{(r)}(x))$  é o registador de deslocamento com comprimento mínimo que produz os síndromas  $S_1, S_2, \dots, S_r$  (este registador de deslocamento pode não ser o único, mas as outras hipóteses têm o mesmo comprimento).

No início da iteração  $r$ , será construída a lista de registadores de deslocamento

$$\begin{array}{c} (L^{(1)}, \Lambda^{(1)}(x)) \\ (L^{(2)}, \Lambda^{(2)}(x)) \\ \vdots \\ (L^{(r-1)}, \Lambda^{(r-1)}(x)) \end{array}$$

O algoritmo de Berlekamp-Massey calcula um novo registo de deslocamento com comprimento mínimo  $(L^{(r)}, \Lambda^{(r)}(x))$  capaz de gerar a sequência  $S_1, S_2, \dots, S_{r-1}, S_r$ . Para obter a nova saída do registador na iteração  $r$ , calcula-se

$$S'_r = -\sum_{j=1}^{N-1} \Lambda_j^{(r-1)} \cdot S_{r-j} \quad (3.35)$$

É de salientar que os termos com grau superior ao de  $\Lambda^{(r-1)}(x)$  são nulos.

Com este objectivo, compara-se em cada iteração  $r$  os síndromas recebidos,  $S_r$ , com os calculados pelo circuito,  $S'_r$ , obtendo-se a “discrepância”

$$\Delta_r = S_r - S'_r = S_r + \sum_{j=1}^{N-1} \Lambda_j^{(r-1)} S_{r-j} = \sum_{j=0}^{N-1} \Lambda_j^{(r-1)} S_{r-j} \quad (3.36)$$

em que  $\Lambda^{(r-1)}(x)$  se refere à iteração precedente.

No caso de  $\Delta_r=0$ ,  $\Lambda(x)$  mantém-se inalterado; se não, altera-se com o objectivo de obter uma discrepância nula, do seguinte modo:

$$\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) - \beta x^u \Lambda^{(n-1)}(x) \quad (3.37)$$

Nesta equação  $\beta$  é um elemento de  $GF(2^m)$ ,  $u$  um número inteiro e  $\Lambda^{(n-1)}$  é o último polinómio que foi obtido em que  $\Delta_n \neq 0$ ; resulta assim uma nova discrepância:

$$\Delta_r' = \sum_{j=0}^{N-1} \Lambda_j^{(r)} S_{r-j} = \sum_{j=0}^{N-1} \Lambda_j^{(r-1)} S_{r-j} - \beta \sum_{j=0}^{N-1} \Lambda_j^{(n-1)} S_{r-j-u} \quad (3.38)$$

Nestas condições, pode especificar-se  $u=r-n$  e  $\beta = \frac{\Delta_r}{\Delta_n}$  de forma a tentar obter um resultado nulo, isto é,

$$\Delta_r' = \Delta_r - \frac{\Delta_r}{\Delta_n} \Delta_n = 0 \quad (3.39)$$

Para realizar este processo de uma forma recursiva, inicializa-se  $\Lambda(x)=B(x)=1$  e  $L=0$ , sendo  $\delta_r=1$  se  $\Delta_r \neq 0$  e  $2L^{(r-1)} < r$  e nulo nos restantes casos, para obter o polinómio  $\Lambda(x)$  após  $2t$  iterações, ficando:

$$L^{(r)} = \delta_r(r-L^{(r-1)}) + (1-\delta_r)L^{(r-1)} \quad (3.40a)$$

$$\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) - \Delta_r x B^{(r-1)}(x) \quad (3.40b)$$

$$B^{(r)}(x) = \Delta_r^{-1} \delta_r \Lambda^{(r-1)}(x) + (1-\delta_r) x B^{(r-1)}(x) \quad (3.40c)$$

$$\Delta_r' = \sum_{j=0}^{N-1} \Lambda_j^{(r-1)} S_{r-j} \quad (3.40d)$$

Depois das  $2t$  iterações, conhecemos o vector  $\Lambda$  e  $2t$  dos  $N$  componentes do vector  $\hat{E} = [E_0 \ E_1 \ \dots \ E_{N-1}]$ :  $E_1=S_1$ ,  $E_2=S_2$ , ...,  $E_{2t}=S_{2t}$ . Para conhecer os restantes componentes do espectro do vector de erros podemos usar de novo o circuito recursivo da figura 3.7, para obter

$$E_k = - \sum_{j=1}^{N-1} \Lambda_j E_{k-j}, \quad k = 2t+1, \dots, N \quad (3.41)$$

(Note-se que  $E_N=E_0$ ).

Assim se pode determinar o vector  $\hat{C} = V - \hat{E}$  e, através da transformada de Fourier inversa, o vector  $\hat{c} = [c_0 c_1 \dots c_{N-1}]$  pretendido. A estimativa do bloco de informação pode então obter-se de imediato, tirando partido da codificação sistemática.

### 3.3.4 Adaptação do algoritmo de Berlekamp-Massey para correcção de erros e rasuras

Para decodificar palavras que contêm rasuras basta preencher as rasuras com símbolos previamente definidos e actualizar o polinómio de localização de erros de forma a incluir as rasuras existentes. Não havendo erros, o código RS pode corrigir até  $2t = N - K$  rasuras, como vimos atrás.

Define-se o “vector de rasuras” como um vector de comprimento  $N$  com componentes  $f_i$ : se existirem rasuras nas localizações  $i_1, i_2, \dots, i_p$  aquele vector tem componentes  $f_{i_n}$ , para  $n=1, 2, \dots, p$ , iguais ao símbolo rasurado, sendo os outros componentes  $f_i$  iguais a zero. Então

$$v_i = c_i + e_i + f_i, \quad i=0, 1, \dots, N-1. \quad (3.42)$$

Seja  $\psi = [\psi_0 \ \psi_1 \ \dots \ \psi_{N-1}]$  um vector com componentes nulos em correspondência com as rasuras e não nulo no caso contrário. Assim

$$\psi_i v_i = \psi_i (c_i + e_i + f_i) = \psi_i c_i + \psi_i e_i \quad (3.43)$$

Devido à possibilidade de rasuras, os componentes do vector recebido são modificados para  $v'_i = \psi_i v_i$ , os do vector de erros para  $e'_i = \psi_i e_i$  e os do vector de código para  $c'_i = \psi_i c_i$ , pelo que

$$\psi_i v_i = v'_i = c'_i + e'_i \quad (3.44)$$

Há agora que descodificar  $\underline{v}=[v_0 v_1 \dots v_{N-1}]$  para achar  $\underline{e}=[e_0 e_1 \dots e_{N-1}]$ .

Para calcular o “polinómio de localização de rasuras” no domínio da frequência define-se  $U_r=\alpha^{i(r)}$ , em que  $i(r)$ , com  $r=1,2,\dots,\rho$ , representa a localização das rasuras. Fica assim

$$\Psi(x)=(1-xU_\rho)(1-xU_{\rho-1})\dots(1-xU_1)=\sum_{k=0}^{N-1} \Psi_k x^k \quad (3.45)$$

Para implementar o cálculo deste polinómio de uma forma recursiva, inicializa-se  $\Psi(x)=1$ , obtendo-se a cada iteração a seguinte equação

$$\Psi^{(r)}(x)=(1-xU_r)\Psi^{(r-1)}(x)=\Psi^{(r-1)}(x)-xU_r\Psi^{(r-1)}(x), \quad r=1,\dots,\rho \quad (3.46)$$

Há que definir os sindromas modificados

$$S'_j=(\Psi*V)_j=(\Psi*C)_j+(\Psi*E)_j=(\Psi*E)_j, \quad j=1,\dots,2t$$

para os  $2t-\rho$  valores de  $j$  para os quais  $(\Psi*C)_j=0$ . (3.47)

Podemos definir um “polinómio de localização de erros e rasuras” combinando os polinómios de localização de erros e de localização de rasuras; procede-se então como se só houvesse erros, com o “polinómio equivalente de localização de erros”  $\Lambda'(x)=\Lambda(x)\Psi(x)$ . Este polinómio é nulo no domínio do tempo ( $\lambda'_i=0$ ) sempre que haja erros ou rasuras; ficando  $\lambda'_i(e_i+f_i)=0$ , resulta no domínio da frequência  $(\Lambda'*(E+F))=0$ . Como num bloco de comprimento  $2t$  são conhecidos os valores de  $(E_j+F_j)$ , obtém-se a palavra enviada  $C_j=V_j-(E_j+F_j)$ , recursivamente.

Para calcular este polinómio de localização de erros e rasuras  $\Lambda'(x)$  pode usar-se o algoritmo de Berlekamp-Massey ficando:

$$\Lambda'(x)=\Lambda^{(r)}(x)\Psi(x)=\Lambda^{(r-1)}(x)\Psi(x)-\Delta_r x B^{(r-1)}(x)\Psi(x) \quad (3.48a)$$

$$B^{(r)}(x)\Psi(x)=\Delta_r^{-1} \delta_r \Lambda^{(r-1)}(x)\Psi(x)+(1-\delta_r)x B^{(r-1)}(x)\Psi(x) \quad (3.48b)$$

Para calcular a discrepância substitui-se o polinómio de localização de erros ( $\Lambda_j$ ) pelo respectivo polinómio de localização de erros modificado ( $\Lambda'_j$ ), resultando:

$$\Delta_r = \sum_{j=0}^{N-1} \Lambda'_j{}^{(r-1)} S_{r-j} \quad (3.49)$$

Substituindo agora a notação  $\Lambda'_j(x)$  por  $\Lambda_j(x)$ , o polinómio de localização de erros e rasuras vai ser inicializado com  $\Lambda(x)=B(x)=\Psi(x)$  em vez de "1", gerando recursivamente as equações:

$$\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) - \Delta_r x B^{(r-1)}(x) \quad (3.50a)$$

$$B^{(r)}(x) = \Delta_r^{-1} \delta_r \Lambda^{(r-1)}(x) + (1 - \delta_r) x B^{(r-1)}(x) \quad (3.50b)$$

$$\Delta_r = \sum_{j=0}^{N-1} \Lambda_j{}^{(r-1)} S_{r-j} \quad (3.50c)$$

Para implementar o algoritmo de descodificação de forma a incluir a localização das rasuras, basta acrescentar um bloco de rasuras para inicializar  $\Lambda(x)=\Psi(x)$ . Podemos estabelecer as seguintes correspondências com a forma inicial do algoritmo:

$$2L^{(r-1)} < r \leftrightarrow 2(L^{(r-1)} - \rho) < r - \rho \leftrightarrow 2L^{(r-1)} < r + \rho \quad (3.51a)$$

$$L^{(r)} = r - L^{(r-1)} \leftrightarrow L^{(r)} - \rho = r - \rho - (L^{(r-1)} - \rho) \leftrightarrow L^{(r)} = r - L^{(r-1)} + \rho \quad (3.51b)$$

A implementação do algoritmo de descodificação de Berlekamp-Massey está ilustrada no fluxograma da figura 3.8. É de salientar que só se recorre ao bloco de rasuras no caso da serem indicadas rasuras na palavra recebida.

Uma questão crucial há ainda a referir: e se o número de erros  $t'$  e rasuras  $\rho$  não verificar a relação  $2t' + \rho + 1 \leq d_{\min}$  (por exemplo,  $t' > t$  quando  $\rho=0$ )?

Neste caso, não é forçoso que surja um erro de descodificação (o código RS não é aquilo a que se chama um "código perfeito" [10]), ainda que não haja garantias de evitar esse erro. Ignorando o descodificador, de facto, o verdadeiro  $t'$ , uma forma

prática de reduzir os erros de descodificação é renunciar à descodificação completa quando ela implica um  $t'$  estimado tal que  $2t'+\rho+1 > d_{\min}$ ; nessas situações, o descodificador limita-se a assinalar uma falha na descodificação, isto é, detecta erros sem os corrigir. O algoritmo de Berlekamp-Massey adapta-se bastante bem a esta estratégia. Basta que, uma vez calculado o polinómio  $\Lambda(x)$ , se verifique se  $S_j = S_{((N+j))}$ , para  $j=1,2,\dots,2t$ , com

$$S_j = \sum_{i=1}^L \Lambda_i S_{j-i}, \quad j=2t+1,\dots,N+2t \quad (3.52)$$

em que  $L$  designa o grau de  $\Lambda(x)$ .

Caso contrário, renuncia-se à descodificação, sendo assinalada a respectiva falha [10].

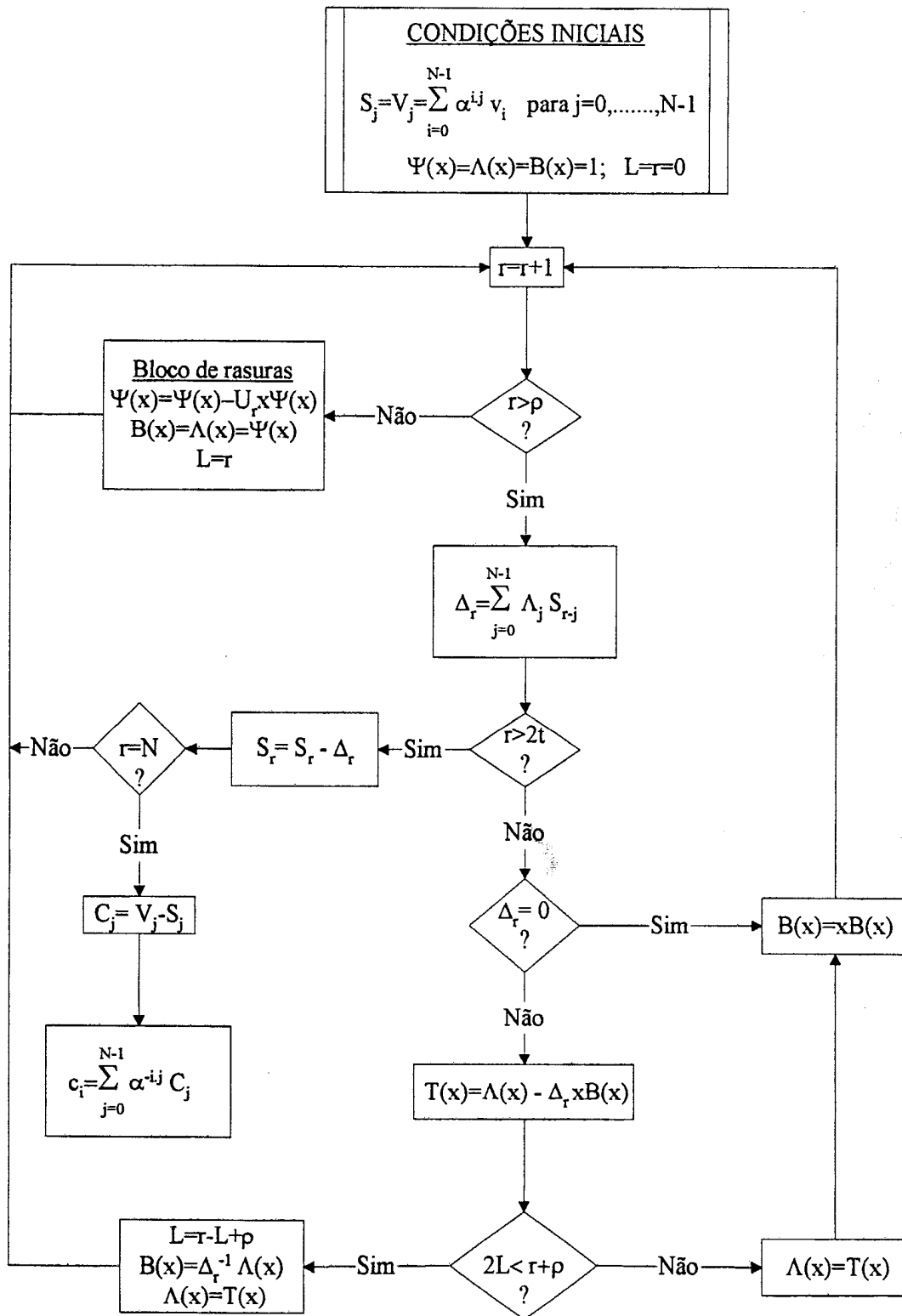


Figura 3. 8: Decodificador de Berlekamp-Massey.

# Capítulo 4

## AVALIAÇÕES DE DESEMPENHO

Referimos no capítulo 2 algumas das características da radiotransmissão no âmbito do sistema MBS, tendo identificado os principais requisitos e restrições. O trabalho realizado para fins de preparação desta tese usou como ponto de partida, no que se refere a avaliações de desempenho, um conjunto de resultados relativos à transmissão em ambientes exteriores (onde o canal pode ser particularmente hostil), obtidos a nível do projecto RACE/MBS; alguns destes resultados foram já aqui referidos (na secção 2.2), dizendo respeito a um cenário de transmissão considerado em [3]. As avaliações de desempenho que levámos a cabo, partindo de resultados como os citados em [3], incluíram a estratégia de controlo de erros proposta no capítulo 3, permitindo ajuizar quanto ao respectivo impacto; permitiram ainda tirar algumas conclusões sobre a razoabilidade de diversas escolhas no tocante às características das antenas e das estruturas celulares, em ligação com estimativas dos requisitos de potência para que a qualidade de serviço esteja assegurada.

A secção 4.1 é dedicada às condições de simulação, com indicação do cenário respectivo, de diversas opções de implementação entre as consideradas em [3], e ainda da metodologia da simulação, pelo método de Monte-Carlo. Na secção 4.2 apresentam-se múltiplos resultados numéricos, para as opções acima referidas e diversos “limiares” no quadro da estratégia de controlo de erros; finalmente, na secção 4.3, estes resultados são detalhadamente discutidos, no sentido de traçar algumas conclusões.

## 4.1 CONDIÇÕES DE SIMULAÇÃO

### 4.1.1 Cenário de simulação

A figura 4.1 diz respeito ao cenário de simulação, já adoptado em [3], que consiste numa “típica” rua de cidade, limitada por edifícios distando 30m. A antena da BS é directiva e não ilumina a região mais próxima (admite-se que esta é iluminada por outra BS, como vimos na figura 2.3-B), e a presença de um autocarro nas imediações dá origem a percursos de propagação adicionais entre a BS e a MS. A contribuição dos raios reflectidos pelo autocarro para os parâmetros de propagação depende da distância  $d$  e do diagrama de radiação da antena usada no móvel.

Nas condições referidas, a figura 4.2 dá-nos os valores do *delay spread* não excedidos durante 90% do tempo, quando são usadas antenas omnidireccionais no móvel, tanto para polarização vertical (V) como circular (C). Supõe-se que estas são antenas bicónicas com largura de feixe de  $20^\circ$  no plano vertical. A outra opção considerada para a antena do móvel é um esquema de feixes comutáveis, com selecção de feixe na base da potência média recebida e largura do mesmo de  $40^\circ$  e  $20^\circ$ , respectivamente, nos planos horizontal e vertical. Com estas antenas directivas, e com polarização vertical, o *delay spread* é da ordem dos 20ns, não dependendo da distância  $d$  pois o diagrama de radiação da antena directiva praticamente suprime o efeito dos raios reflectidos pelo autocarro. Admite-se ainda que a estação móvel se desloca paralelamente ao eixo da rua, com uma velocidade de 50km por hora.

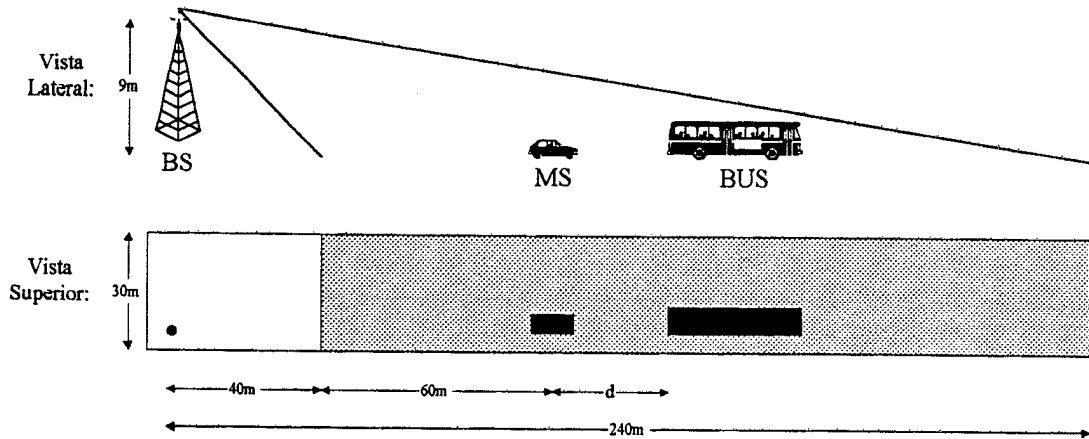


Figura 4. 1: Cobertura da BS no cenário de simulação.

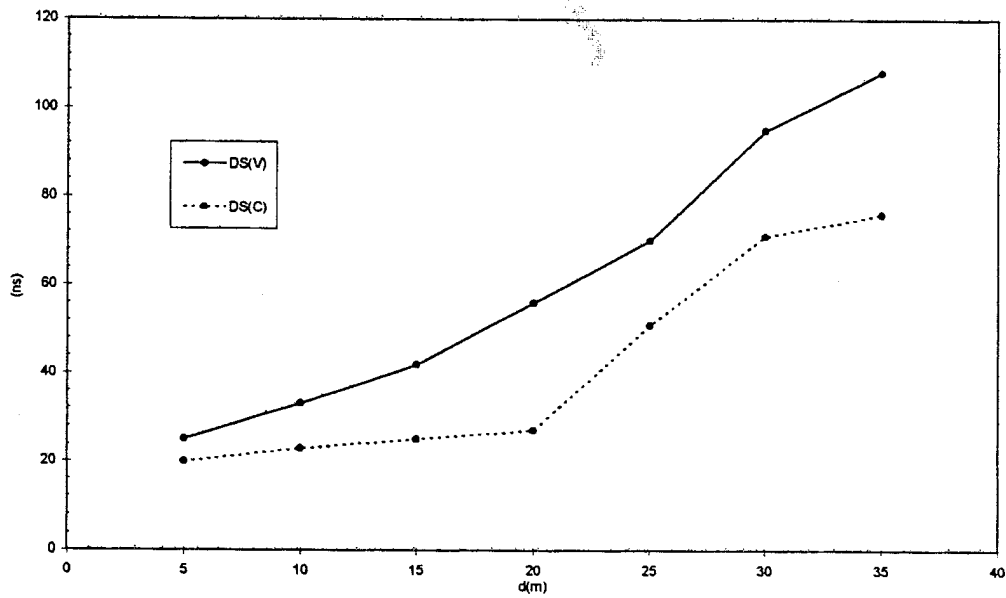


Figura 4. 2: Parâmetros de dispersão (*delay spread*):  
 DS(V): Antena omnidireccional com polarização vertical.  
 DS(C): Antena omnidireccional com polarização circular.

#### 4.1.2 Opções de implementação quanto a igualização e diversidade

Das diversas opções de implementação consideradas em [3] seleccionamos as seguintes:

- Três hipóteses quanto à antena da MS: omnidireccional com polarização vertical, omnidireccional com polarização circular, directiva com feixes comutáveis e polarização vertical.
- Modulação e desmodulação 4-OQAM série, com um *gross bit rate* de 40Mbps.
- Um DFE (3,5) e um DFE (9,11), respectivamente, quando se usam na MS as antenas de feixes comutáveis e as antenas omnidireccionais; um algoritmo de seguimento “complexo” com coeficiente de adaptação  $\Delta=0.01$  [2,3].
- Diversidade espacial dupla por selecção de antena na base da potência máxima recebida.

#### 4.1.3 Metodologia da simulação

A metodologia adoptada para a avaliação do desempenho do sistema, por simulações pelo método de Monte-Carlo, teve em conta os seguintes aspectos:

- No que se refere a um dado *burst* (por exemplo *standard*), a simulação do processo de igualização consome muito mais tempo que a do processo de descodificação interna (com o algoritmo indicado na secção 3.2.1.2), e esta muito mais tempo do que o processo de descodificação externa (com os algoritmos descritos na secção 3.3).
- As probabilidades de erro residuais após a descodificação externa são muito mais baixas que as probabilidades de erro nas decisões do DFE, sendo

intermédios os valores das probabilidades de erro nas decisões do decodificador interno.

Face ao que acabamos de referir, entendemos levar a cabo o processo de simulação em três etapas, distintas e sucessivas, relacionadas com as operações de igualização, descodificação interna e descodificação externa, respectivamente. O objectivo foi reduzir tanto quanto possível o tempo total de simulação, mas garantindo ao mesmo tempo estimativas de desempenho razoavelmente precisas.

Numa primeira etapa, simulam-se as operações de igualização para um certo número de *bursts* (tanto maior quanto maior o valor de  $\frac{\bar{E}_b}{N_c}$ , para obter precisão similar), o que produziu distribuições de erros como as referidas no capítulo 2. Numa segunda etapa, as distribuições de erros na saída do decisor do DFE (decisões binárias consoante a polaridade) são usadas para caracterizar estatisticamente as flutuações do “canal”, assim permitindo gerar amostras na entrada daquele decisor (entrada também do decodificador interno) referentes a um número de *bursts* significativamente mais elevado que o considerado na simulação da igualização; obviamente as amostras são tais que as decisões tomadas sobre elas, consoante a polaridade, conduzem aproximadamente às distribuições de erros da primeira etapa. Esta etapa produz distribuições de erros e rasuras em sextetos de bits (símbolos RS) que são usadas na etapa seguinte. Na terceira etapa, o processo de descodificação externa (RS(42,36) e, quando necessário RS(60,36)), é realizado para um número muito elevado de *bursts*, gerados com base nas distribuições de erros e rasuras obtidas na etapa anterior.

Uma medida, mais ou menos óbvia, que foi adoptada para reduzir o tempo de simulação, no quadro do “método das três etapas”, consistiu em não realizar a descodificação interna para *bursts* sem erros nas decisões do DFE (no fundo, a maioria dos *bursts*, atendendo à figura 2.5); admitiu-se, logicamente, que a descodificação não produziria nunca qualquer erro ou rasura nestes *bursts*, cujo peso percentual foi tido em conta nas estimativas de desempenho global. Por motivos análogos, não foi realizada a descodificação externa para *bursts* sem qualquer erro e/ou rasura nas decisões do decodificador interno.

Um dos objectivos do nosso trabalho de simulação foi avaliar as potencialidades da estratégia de controlo de erros proposta, no que diz respeito aos compromissos

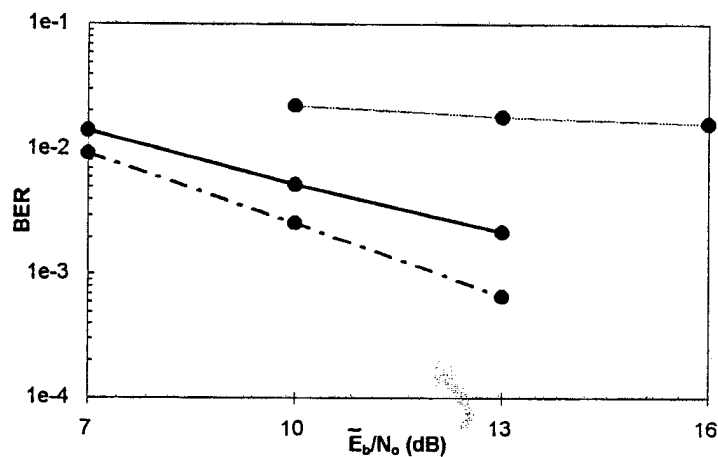
atingíveis entre “probabilidade de erro residual” e “atraso de descodificação”. Este atraso está ligado ao peso relativo das transmissões adicionais requeridas para recuperar cada célula ATM, mas também depende de factores fora do âmbito desta tese, por exemplo o esquema MAC (Medium Access Control) a utilizar, etc. Optou-se por considerar a manutenção do “estado” do canal nas primeiras transmissões dos *bursts* médios complementares, de modo a testar a capacidade da estratégia de controlo de erros para lidar com períodos “longos” (digamos, mais de dez tramas, isto é, 7.68ms) de condições de transmissão “moderadamente más”, mantendo um pequeno “atraso de descodificação”. Admitiu-se ainda que as mensagens ACK e NAK, enviadas em *bursts* curtos de controlo, não são afectadas por erros de descodificação, graças a uma protecção específica adicional.

## **4.2 Resultados numéricos**

Os resultados numéricos que a seguir apresentamos foram obtidos por simulação pelo método de Monte-Carlo, de acordo com a metodologia exposta na secção 4.1, e dizem respeito ao cenário de simulação e às opções de implementação que nessa secção são descritos.

Começamos por resultados referentes à operação de igualização, primeira etapa do processo de simulação, para uma distância  $d=30\text{m}$  entre a estação móvel e o autocarro “perturbador” (Ver figura 4.1). Considerou-se a hipótese, realista, de um *offset* de frequência de 0.15 ppm afectando o desempenho do igualizador. A figura 4.3 dá conta dos resultados obtidos com as três opções alternativas quanto à antena da MS e as opções complementares referidas na secção 4.1.2 no que diz respeito à taxa de erros média nas decisões do DFE (decisões binárias:  $\pm 1$ ). Note-se que há, de *burst* para *burst*, flutuações significativas em torno destes valores médios; as distribuições de erros da figura 2.5 referem-se precisamente à situação que, em termos médios, se traduz pela linha a traço-ponto da figura 4.3, e que diz respeito à antena directiva com polarização vertical.

Como se pode ver na figura 2.5, muitos dos *bursts* têm um pequeno número ou mesmo uma completa ausência de erros; só numa pequena fracção dos *bursts* simulados foi elevado o número de erros. Contudo, há que notar que as distribuições de erros dependem fortemente de  $\frac{\bar{E}_b}{N_0}$  ( $\bar{E}_b$  e  $N_0$  designam, respectivamente, o valor médio da energia por bit e a densidade espectral de potência do ruído equivalente na entrada do desmodulador); é obvio que quanto mais baixos forem os valores de  $\frac{\bar{E}_b}{N_0}$ , mais elevadas se tornam as percentagens de *bursts* “relativamente maus” e “muito maus”.

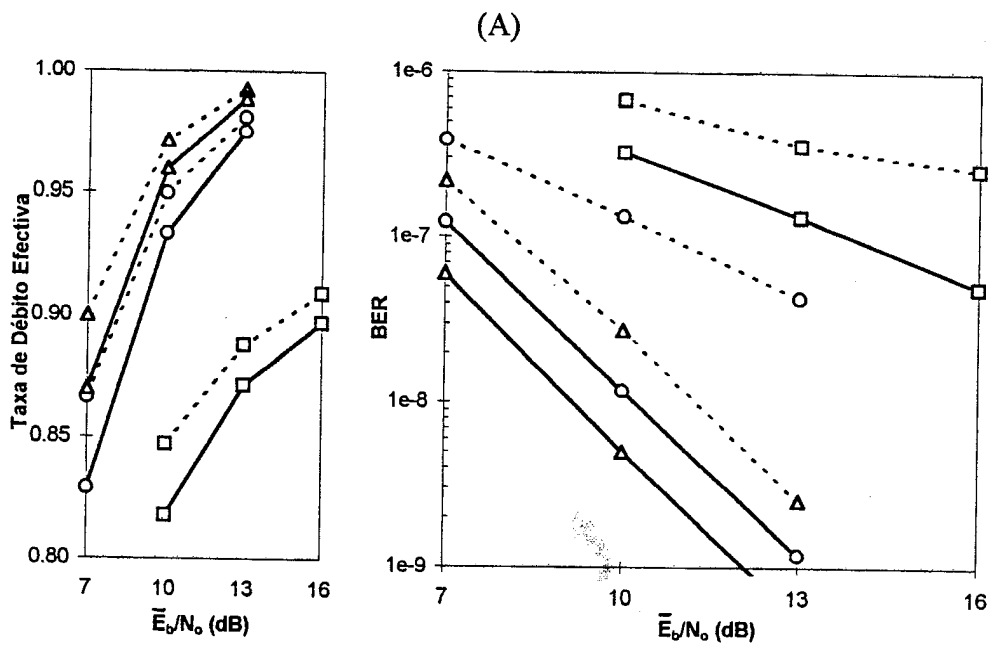


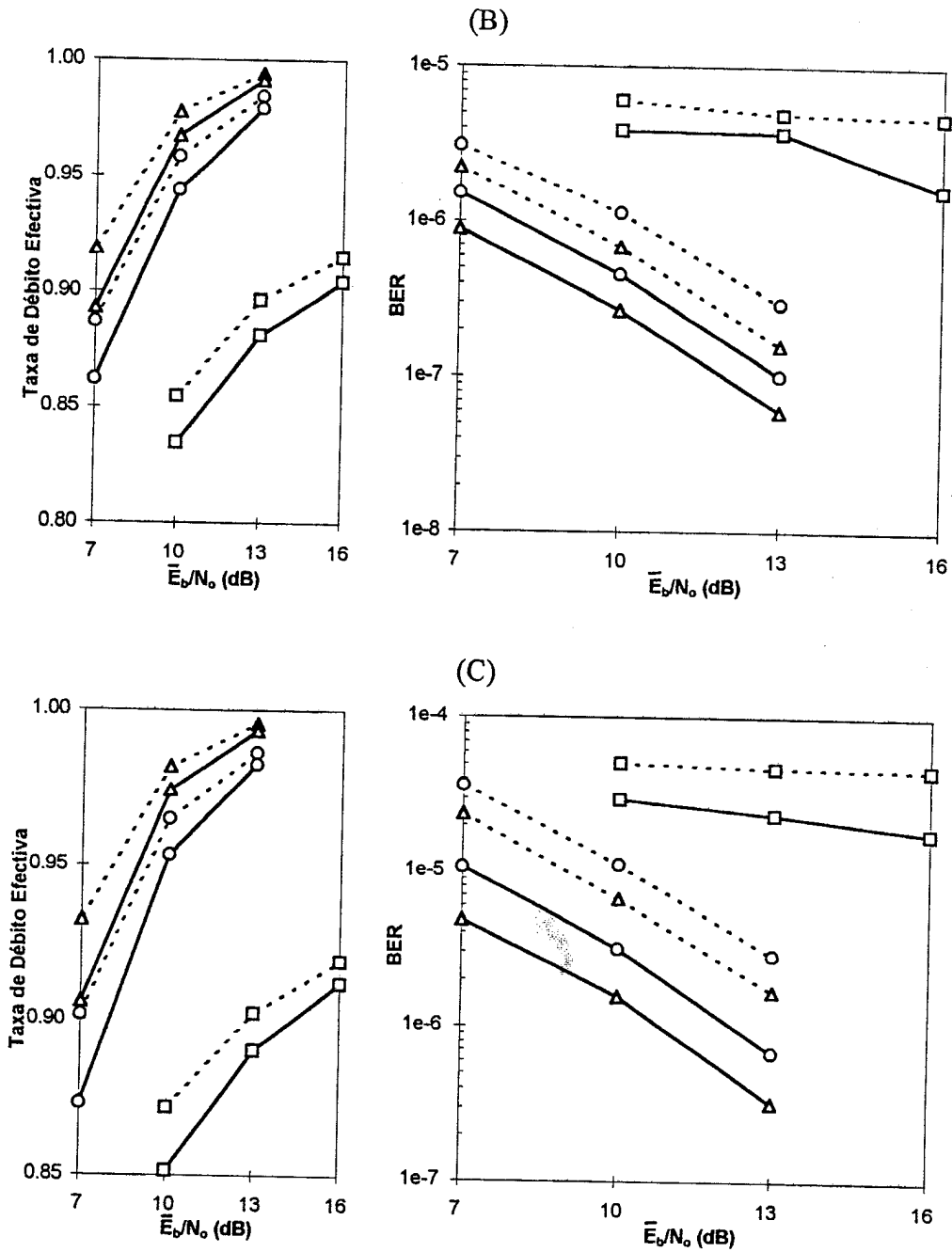
**Figura 4. 3: Desempenho do DFE com as seguintes antenas:**  
 Tracejado - Antena omnidireccional com polarização vertical.  
 Cheio - Antena omnidireccional com polarização circular.  
 Traço e ponto - Antena directiva com polarização vertical.

As simulações que incluem a descodificação de canal, de acordo com a estratégia de controlo de erros proposta no capítulo 3, foram realizadas para várias combinações de dois limiares internos ( $L=1.6$  e  $L=2.1$ ) e três pares de limiares externos ( $L_1=0$  e  $L_2=6$ ;  $L_1=2$  e  $L_2=8$ ;  $L_1=4$  e  $L_2=10$ ). Com estes limiares foram obtidas não só as probabilidades de erro (BER) residuais, após a descodificação, como também as “taxas de débito efectivas” correspondentes. A “taxa de débito efectiva” é aqui definida como a razão entre o número mínimo de *slots standard* requeridos para transmitir um certo número de células ATM (admitindo ausência de transmissões adicionais) e o número de *slots standard* efectivamente ocupados, maior que o primeiro devido às

transmissões adicionais no âmbito da estratégia de controlo de erros; note-se que, como vimos no capítulo 2, dois *slots* médios equivalem a um *slot standard*.

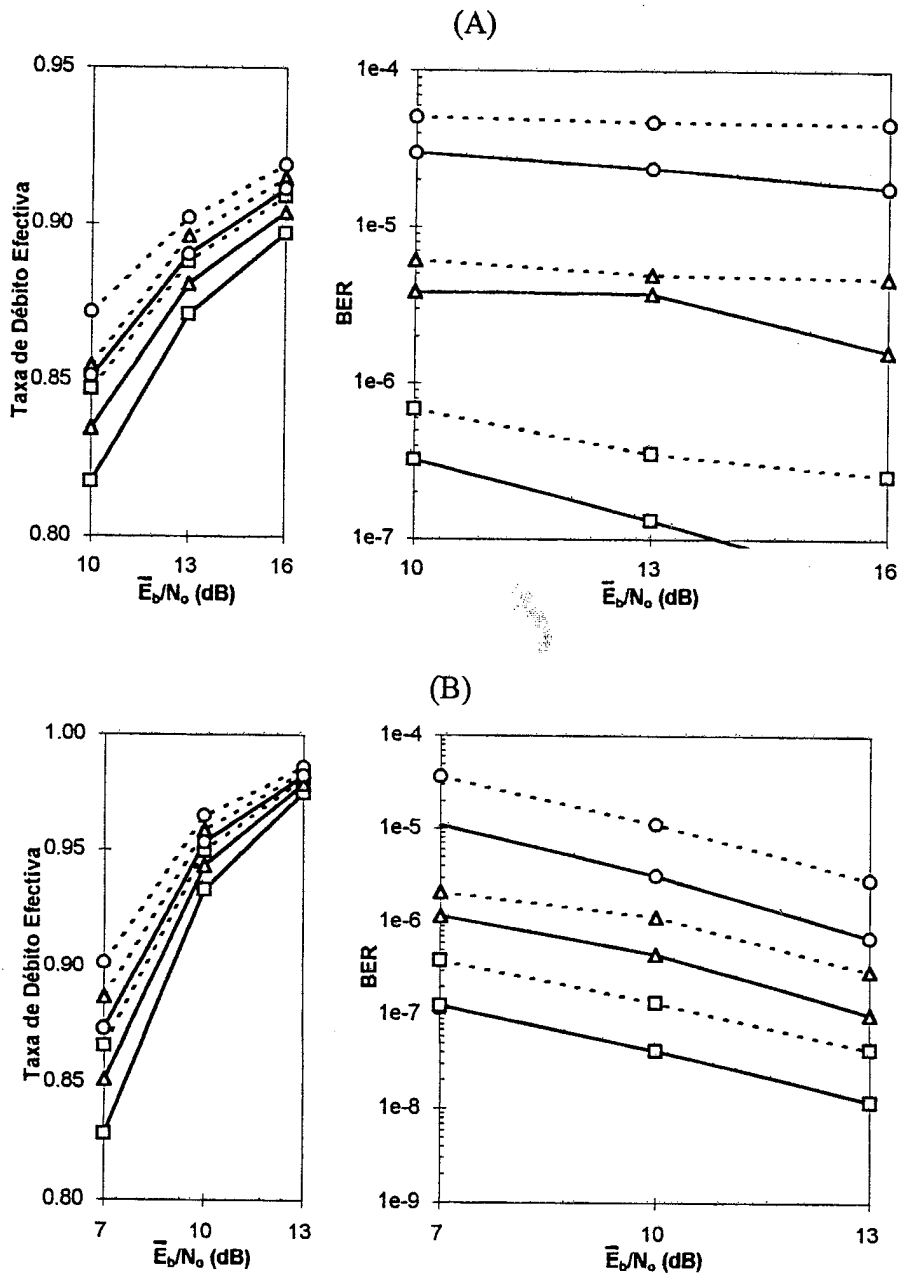
Os resultados obtidos podem ver-se na figura 4.4 (A), (B) e (C), para as várias combinações dos limiares escolhidos, e as três opções de implementação atrás indicadas (antenas, etc.), com a MS colocada a 100m da BS e o autocarro a 30m daquela.

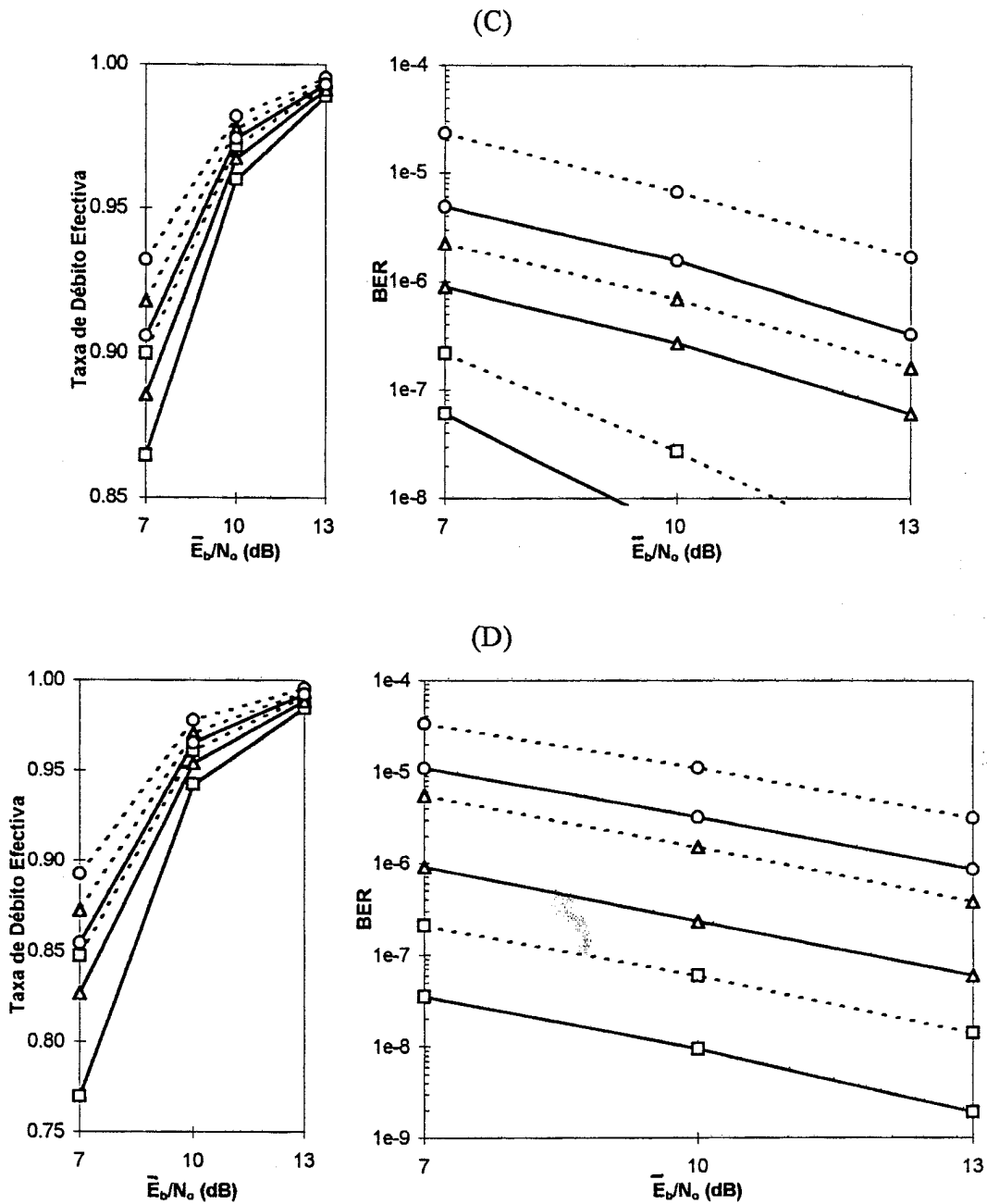




**Figura 4. 4: Desempenhos para diferentes limiares e antenas**  
**Limiars externos: (A)  $L_1=0$  e  $L_2=6$ ; (B)  $L_1=2$  e  $L_2=8$ ; (C)  $L_1=4$  e  $L_2=10$**   
**Limiar interno: 1.6 (Tracejado) ou 2.1 (cheio)**  
 Retângulo: Antena omnidireccional com polarização vertical  
 Círculo: Antena omnidireccional com polarização circular  
 Triângulo: Antena directiva com polarização vertical

A figura 4.5 mostra os mesmos resultados que a figura 4.4 ((A), (B) e (C)), mas organizados de forma diferente, facilitando outras comparações. Na figura 4.5 (D) mostram-se também resultados para a MS a 240m da BS, i.e., no "limite da célula", equipada com antena directiva e polarização vertical (não foi considerado o autocarro neste caso).





**Figura 4. 5: Desempenhos para os seguintes casos:**

(A) Antena omnidireccional com polarização vertical a 100m da BS

(B) Antena omnidireccional com polarização circular a 100m da BS

(C) Antena directiva com polarização vertical a 100m da BS

(D) Antena directiva com polarização vertical a 240m da BS

Limiar interno:  $L=1.6$  a tracejado e  $L=2.1$  a cheio

Limiar externo: Rectângulo ( $L_1=0$  e  $L_2=6$ ), Triângulo ( $L_1=2$  e  $L_2=8$ ) e

Círculo ( $L_1=4$  e  $L_2=10$ )

Para entender melhor o papel desempenhado pelos limiares externos considerou-se o esquema de controlo de erros com o fluxograma representado na figura 4.6 que conduz aos resultados (nitidamente inferiores) que a figura 4.7 indica.

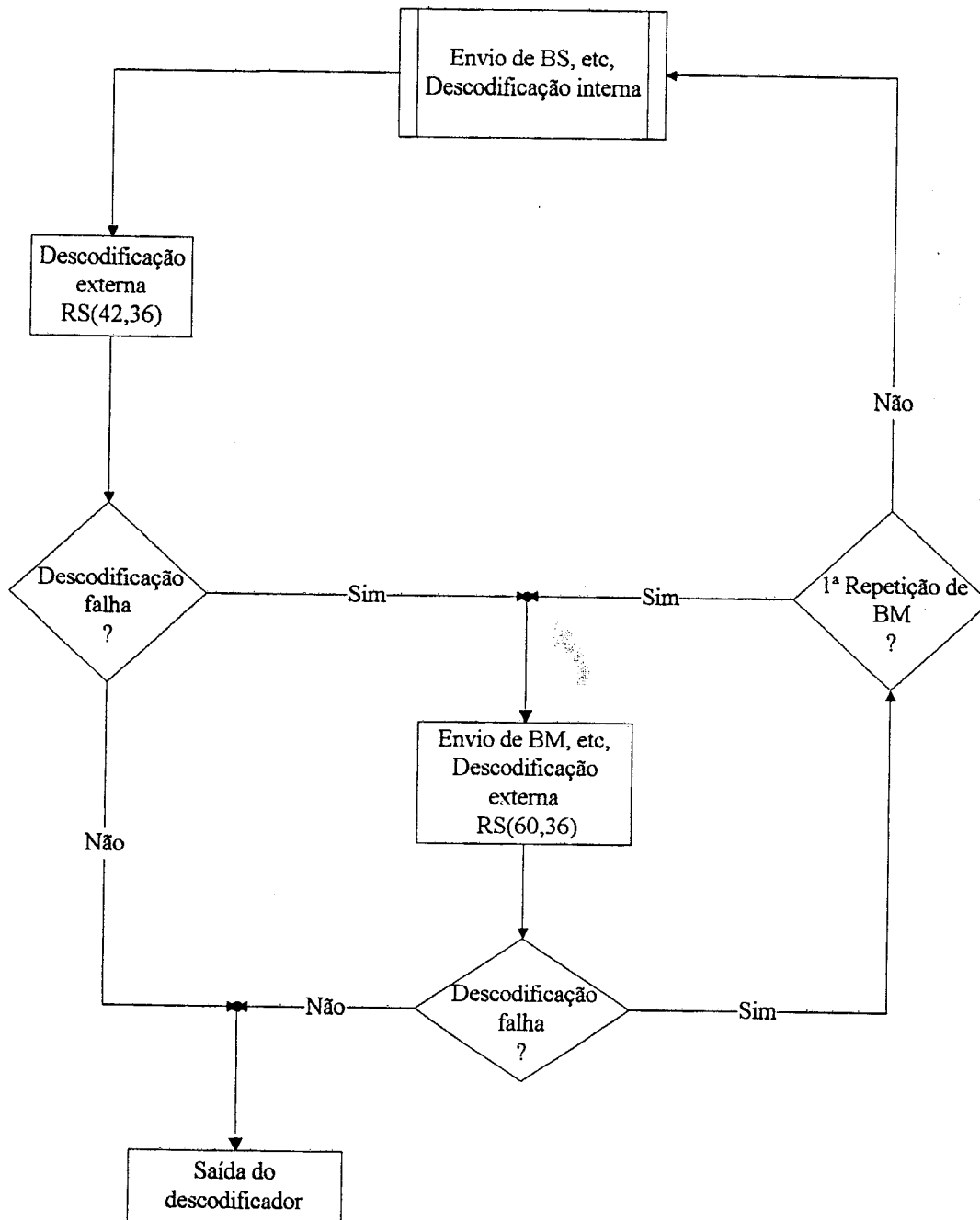
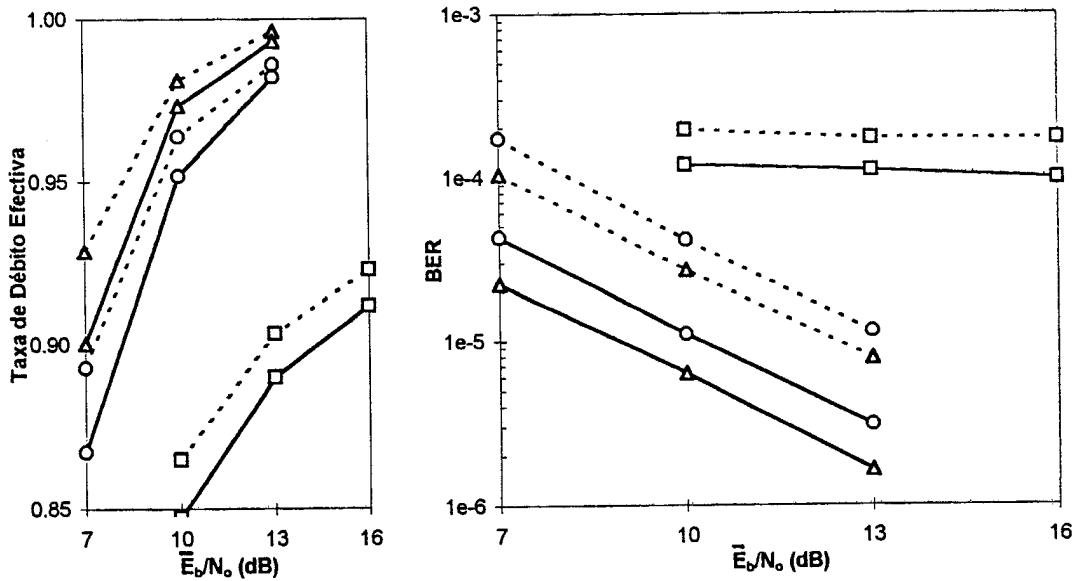


Figura 4. 6: Fluxograma dum esquema de controlo de erros sem utilização de limiares externos.



**Figura 4. 7: Desempenhos sem utilização de limiares externos:**  
 Rectângulo: Antena omnidireccional com polarização vertical  
 Círculo: Antena omnidireccional com polarização circular  
 Triângulo: Antena directiva com polarização vertical

### 4.3 Discussão dos resultados obtidos

Os resultados obtidos permitem formar uma ideia sobre as potencialidades da estratégia de controlo de erros proposta nesta tese, e, ao mesmo tempo, dão indicações importantes sobre opções de implementação desejáveis, nomeadamente no que diz respeito a antenas.

Começamos pela figura 4.3, que, desde logo, nos sugere que é vantajoso adoptar antenas directivas na MS (esquemas de feixes comutáveis), ou, em alternativa, adoptar polarização circular se as antenas da MS forem omnidireccionais; a vantagem resulta da eliminação, total (antena directiva) ou parcial (polarização circular), dos raios reflectidos pelo autocarro, o que diminui o *delay spread*, como vimos na secção 4.1.1. Usando polarização vertical, o desempenho do DFE com antenas omnidireccionais na MS é bastante pior que o obtido com antenas directivas, apesar da significativamente maior complexidade de igualização ( DFE (9,11) face a DFE (3,5) ); mesmo aumentando bastante o valor de  $\frac{\bar{E}_b}{N_0}$ , é praticamente impossível alcançar uma

probabilidade de erro média inferior a  $10^{-2}$ . As figuras 4.4 (A), (B) e (C) confirmam estas vantagens: sejam quais forem os limiares  $L$  (interno),  $L_1$  e  $L_2$  (externos) escolhidos, o desempenho é melhor com antenas directivas que com as omnidireccionais, e a polarização circular é vantajosa relativamente à polarização vertical. As vantagens são nítidas, quer em termos de probabilidade de erro residual, quer em termos da taxa de débito efectiva. As figuras 4.4 e, de forma mais directa, 4.5 (A), (B) e (C) mostram ainda que o aumento do limiar interno e a redução dos limiares externos tendem a reduzir a probabilidade de erro residual, mas, em contrapartida, tendem a diminuir a taxa de débito efectiva. A diminuição desta taxa está associada a um aumento das transmissões adicionais, sejam elas para enviar *bursts* médios complementares ou para repetir os *bursts standard*; com uma elevada percentagem de transmissões adicionais é dificilmente evitável um significativo atraso na descodificação. Note-se aliás que, mesmo com a pior solução quanto às antenas (omnidireccionais com polarização vertical), é possível chegar a probabilidades de erro residuais inferiores a  $10^{-6}$ , apesar da probabilidade de erro superior a  $10^{-2}$  nas decisões do DFE; contudo, as taxas de débito efectiva são então bastante baixas, mesmo para valores relativamente elevados de  $\frac{\bar{E}_b}{N_0}$ .

A figura 4.5 (D), referente apenas à opção das antenas directivas na MS, numa situação de transmissão na “fronteira” da célula, é directamente comparável com a figura 4.5 (C), referente à mesma opção e a uma distância menor entre a BS e a MS. A degradação (moderada) a que se assiste é explicável pelos valores mais elevados do *delay spread*, que originam probabilidades de erro no DFE (3,5) de  $1.14 \times 10^{-2}$ ,  $3.12 \times 10^{-3}$  e  $7.78 \times 10^{-4}$ , para  $\frac{\bar{E}_b}{N_0} = 7, 10$  e  $13$  dB, respectivamente..

Repare-se ainda, comparando a figura 4.7 com as figuras 4.4 e 4.5, como é evidente a vantagem da estratégia de controlo de erros proposta relativamente à estratégia que “dispensa” os limiares externos, patente no fluxograma da figura 4.6. Repare-se também que, com uma escolha adequada dos limiares de descodificação interna e externa, é possível uma transmissão de qualidade para um ritmo útil (SBR) de 17Mbps, mesmo com  $\frac{\bar{E}_b}{N_0} \approx 7$  dB: sem transmissões adicionais associadas ao controlo de erros,

este ritmo significa a ocupação de  $34/40=0.85$  da trama (ver secção 2.1); obviamente que uma taxa de débito efectiva não inferior a 0.85 satisfaz o objectivo.

De uma maneira geral, pode dizer-se que a estratégia de controlo de erros que aqui propomos permite um boa qualidade de serviço, para uma ampla gama de serviços possíveis, mesmo quando a qualidade do canal atravessa períodos “longos” em que se apresenta relativamente baixa. Os limiares (interno e externos) adoptados na descodificação podem ser ajustados no início da transmissão em função dos requisitos do serviço em causa (probabilidade de erro residual pretendida, atraso tolerável, etc.); podem ainda ser ajustados durante a transmissão, tendo em conta o estado do canal e mesmo as condições de tráfego.

Para terminar esta secção, voltamos ao problema da escolha das antenas para os móveis. Aparentemente, só a combinação “antenas omnidireccionais”/polarização vertical” é de rejeitar. As outras duas opções produzem resultados não muito diferentes, e, se é verdade que as antenas directivas permitem um melhor desempenho, convirá não esquecer que a sua implementação é mais dispendiosa (e as dimensões superiores) quando comparadas com as antenas omnidireccionais com polarização circular.

Para uma comparação mais justa entre as opções “aceitáveis” teremos que ter em conta, não só os desempenhos em função de  $\frac{\bar{E}_b}{N_o}$ , mas também outros aspectos, nomeadamente as relações entre a potência média recebida,  $P_R$ , e a potência média transmitida,  $P_T$ . O valor de  $P_T$  requerido depende não só do valor de  $\frac{\bar{E}_b}{N_o}$  requerido mas também da relação  $\frac{P_R}{P_T}$  (que é significativamente mais favorável com antenas directivas que com antenas omnidireccionais), entre outros factores. Pode dizer-se que:

$$\begin{aligned} P_T(\text{dBm}) &= \frac{\bar{E}_b}{N_o}(\text{dB}) - \frac{P_R}{P_T}(\text{dB}) + 10 \cdot \log_{10}(R_b) + KT(\text{dBm}) + F(\text{dB}) + M(\text{dB}) = \\ &= \frac{\bar{E}_b}{N_o}(\text{dB}) - \frac{P_R}{P_T}(\text{dB}) + 76\text{dB} - 174\text{dBm} + F(\text{dB}) + M(\text{dB}) \end{aligned}$$

em que  $F$  designa o factor de ruído do receptor,  $M$  é uma margem do sistema (referente ao *shadowing*, imperfeições de implementação, etc.),  $K$  é a constante de Boltzmann e se admite que  $T \approx 290^\circ\text{K}$ .

No nosso caso, para uma avaliação justa dos méritos relativos das antenas directivas e das omnidireccionais com polarização horizontal, teríamos que atender quer aos requisitos de  $\frac{\bar{E}_b}{N_0}$  (o que foi já feito nesta secção), quer aos valores de  $\frac{P_R}{P_T}$ , de modo a comparar os requisitos de potência transmitida para iguais valores de  $F$  e de  $M$ . Determinados os valores de  $\frac{P_R}{P_T}$ , torna-se muito clara a vantagem das antenas directivas: com efeito, na situação em que a distância do móvel à base é de 100m, os valores aproximados desta relação são -84 dB e -77 dB, respectivamente, para as antenas omnidireccionais com polarização circular e para as antenas directivas. A esta vantagem de cerca de 7 dB para as antenas directivas há que adicionar a vantagem em termos de  $\frac{\bar{E}_b}{N_0}$ , patente nas figuras 4.4 e 4.5.

É importante estimar os níveis de potência transmitida que são requeridos na "fronteira" da célula (MS a 240m da BS) quando se empregam as antenas directivas na MS. Neste caso,  $\frac{P_R}{P_T} = -84$  dB (semelhante ao que tínhamos com antenas omnidireccionais a 100m). Sendo  $\frac{\bar{E}_b}{N_0} \approx 11$  dB para um dado serviço (Ver figura 4.5 (D)),  $F \approx 9$  dB e  $M \approx 10$  dB (valores realistas a 60GHz), resulta  $P_T \approx 16$  dBm. Sendo definido o objectivo de garantir uma potência de emissão não superior a 100mW para um alcance de pelo menos 200m, pode dizer-se que ele é claramente atingido.

# Capítulo 5

## CONCLUSÕES E PERSPECTIVAS DE TRABALHO FUTURO

O trabalho apresentado nesta tese esteve estreitamente ligado às actividades do projecto RACE/MBS, que decorreram de 1992 a 1995. Tomou-se como ponto de partida um conjunto de especificações (provisórias) do interface rádio proposto para aquele sistema, bem como um conjunto de resultados referentes ao desempenho de esquemas de igualização/diversidade, com diversos tipos de antenas e em diversos ambientes celulares, nomeadamente exteriores.

O objectivo essencial do trabalho consistiu no desenvolvimento e avaliação de uma estratégia de controlo de erros para a “primeira fase” do sistema MBS. A estratégia em análise é de natureza híbrida (ARQ/FEC), assenta na concatenação de um código interno convolucional e um código de blocos externo, não binário, e combina capacidades de correcção e detecção de erros de uma forma adaptativa, sob uma avaliação implícita do estado do canal. Ela assume transmissões adicionais selectivas, que, consoante o “estado” anterior do canal, podem ser de dois tipos: transmissões de redundância adicional para melhorar a capacidade de correcção de erros, com aproveitamento dos dados inicialmente recebidos sob condições de transmissão “intermédias”; retransmissões convencionais, com rejeição dos dados inicialmente recebidos sob condições de transmissão bastante deficientes.

A avaliação da estratégia de controlo de erros proposta foi levada a cabo mediante simulações de Monte-Carlo, de acordo com uma metodologia que visou compatibilizar uma boa precisão com um tempo de computação o mais baixo possível. Isto levou a que o processo de simulação envolvesse três etapas, distintas e sucessivas, relacionadas com as operações de igualização, descodificação interna e descodificação externa.

Os resultados obtidos mostram que a estratégia de controlo de erros proposta, além da sua compatibilidade com as características do ATM e as especificações preliminares

do sistema MBS, apresenta a flexibilidade suficiente para se adaptar a uma ampla gama de serviços e condições de canal. De uma maneira geral, pode dizer-se que resiste bem a más condições de transmissão e que permite uma boa qualidade de serviço mesmo quando a qualidade do canal atravessa períodos “longos” em que se apresenta relativamente débil. Os limiares (interno e externos) adoptados na descodificação podem ser ajustados, pelo que a satisfação dos requisitos de uma gama ampla de serviços não implica mais do que a citada concatenação fixa de códigos, pois a recomendável variabilidade reside nesses limiares ajustáveis.

A estratégia proposta é, em suma, eficiente e flexível; além disso, os códigos interno e externo, com os algoritmos de descodificação referidos, são particularmente indicados para aplicações de alto débito.

Os resultados obtidos dão ainda indicações úteis quanto a outras opções de implementação, para além das estritamente associadas aos códigos de controlo de erros. Nomeadamente, fica claro que a adopção de antenas de feixes comutáveis na MS é uma solução que permite excelentes desempenhos mesmo quando se pretendem alcances superiores a 200m, com potências de emissão inferiores a 100mW.

## *Perspectivas de trabalho futuro*

Enunciam-se em seguida alguns dos objectivos de um trabalho futuro no seguimento do que permitiu a elaboração desta tese, e igualmente relativos ao sistema MBS:

- Ajustamento adaptativo dos limiares (interno e externos) durante a transmissão, de acordo com as flutuações do canal, e respectiva optimização tendo em conta as características dos serviços.

- Estudo do impacto de um código interno mais potente que o considerado neste trabalho (por exemplo, um outro código convolucional com  $R=3/4$  mas maior número de estados).
- Consideração de outros códigos externos no âmbito da “família Reed-Solomon”, nomeadamente construídos sobre  $GF(2^8)$ , com uma única palavra de código por *burst standard*.
- Definição de uma estratégia de controlo de erros para uma fase avançada de implementação do sistema (em que, por exemplo, além da modulação 4-OQAM também é utilizada uma modulação 16-OQAM).
- Avaliações de desempenho em que se tenham em conta outros aspectos do interface rádio, nomeadamente os esquemas de “Medium Access Control” (MAC) e de controlo de potência, de modo a obter indicações precisas quanto a tempos de atraso, requisitos de potência, etc.

# Bibliografia

- [1] - L. Fernandes, "Developing a System Concept and Technologies for Mobile Broadband Communications", IEEE Personal Communications Magazine, February 1995.
- [2] - R. Dinis, A. Gusmão, "Adaptive Serial OQAM-Type Receivers for Mobile Broadband Communications", IEEE VTC'95, Chicago, Julho 1995.
- [3] - R. Dinis, A. Gusmão, J. Fernandes, "Performance Evaluation of Equalisation/Diversity Schemes for MBS", RACE Mobile Telecommunications Summit, Cascais, Novembro 1995.
- [4] - P. Torres, C. Caseiro, A. Gusmão, "Adaptive Error Control Coding for a Mobile Broadband System" a apresentar na VTC'96, Atlanta, Maio 1996.
- [5] - A. Gusmão, M. Prögler, "Physical Channel Design for the Mobile Broadband System", RACE Mobile Telecommunications Workshop, Metz, Junho 1993.
- [6] - A. Gusmão, J. Fernandes, R. Dinis, "Performance of MBS Radio Transmission", RACE Mobile Telecommunications Workshop, Amsterdão, Maio 1994.
- [7] - L. Fernandes, P. Smulders, J. Neves, "Simulation Results on mm-wave Indoor Radio Channel Modelling and Comparison with Measurements", RACE Mobile Telecommunications Workshop, Amsterdão, Maio 1994.
- [8] - S. Lin, D. Costello and M. Miller, "Automatic Repeat Request Error Control Schemes", IEEE Personal Communications Magazine, Vol. 12, nº 12, December 1984.
- [9] - R. Deng, D. Costello, "High Rate Concatenated Coding Systems Using Bandwidth Efficient Trellis Inner Codes", IEEE Transactions on Communications, Vol. 37, nº 5, Maio 1989.
- [10] - R. Blahut, "Theory and Practice of Error Control Codes", Addison-Wesley, Maio 1984.

- [11] - C. Mourot, "Low Delay Data Transmission over the ATDMA Air Interface", RACE Mobile Telecommunications Workshop, Amsterdão, Maio 1994.
- [12] - Yu-Ming Wang, Shu Lin, "A Modified Selective-Repeat Type-II Hybrid ARQ System", ICC'81, Colorado, Junho 1981.
- [13] - J. Hagenauer, "Hybrid ARQ/FEC Protocols on Fading Channels Using Rate Compatible Punctured Convolutional Codes", ICC'87, Seattle, Junho 1987.
- [14] - M. Prögler, "MBS Air Interface Principles", RACE Mobile Telecommunications Summit, Cascais, Novembro 1995.
- [15] - J. Cain, G. Clark and J. Geist, "Punctured Convolutional Codes of Rate  $(n-1)/n$  and Simplified Maximum Likelihood Decoding", IEEE Trans., COM-27, January 1974.
- [16] - Y. Yasuda, K. Kashiki, Y. Hirate, "High Rate Punctured Convolutional Codes for Soft Decision Viterbi Decoding", IEEE Trans. Comm., Vol. 32, nº 3, Março 1984.
- [17] - Viterbi, A. J., "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm", IEEE Trans. Inf. Theory, vol. IT-13, April 1967.
- [18] - F. J. Mac Williams, N. J. A. Sloane, "The Theory of Error-Correcting Codes", Bell Laboratories, Murray Hill, 1977.
- [19] - R. Blahut, "A Universal Reed-Solomon Decoder", IBM J. Res. Develop. Vol. 28, nº 2, Março 1984.
- [20] - E. Berlekamp, "Algebraic Coding Theory", McGraw-Hill Book Co., Inc., New York, 1968.
- [21] - J. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Transactions, IT-15, 122-127, 1969.

# ANEXO

## A 1. CÓDIGO RS(7,3) CONSTRUÍDO SOBRE GF(2<sup>3</sup>)

Seja o código RS(2<sup>m</sup>-1, 2<sup>m</sup>-1-2t), construído sobre GF(2<sup>m</sup>), com m=3 e t=2. Os símbolos de código são os indicados na tabela A.1, se adoptarmos na construção de GF(2<sup>3</sup>) o polinómio primitivo p(x)=x<sup>3</sup>+x+1.

Tabela A 1

$\alpha^n$	$x^0 x^1 x^2$
$\alpha^0$	1 0 0
$\alpha$	0 1 0
$\alpha^2$	0 0 1
$\alpha^3$	1 1 0
$\alpha^4$	0 1 1
$\alpha^5$	1 1 1
$\alpha^6$	1 0 1
0	0 0 0

A tabela de “logaritmos de Zech” é, neste caso,

Tabela A 2

Z	L(Z)
1	3
2	6
3	1
4	5
5	4
6	2

Como se pretende que o código tenha uma capacidade correctora de t=2 erros, o polinómio gerador é o seguinte:

$$g(x)=(x-\alpha)(x-\alpha^2)\dots(x-\alpha^{2t})=(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)=x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3$$

Uma forma de efectuar a codificação sistemática do polinómio de informação  $i(x)=\alpha^6x+\alpha^6$  é construindo o polinómio de código

$$c(x) = i(x) + x^3s(x) = \alpha^4x^6 + \alpha^4x^4 + \alpha^3x^3 + \alpha^6x + \alpha^6$$

em que  $s(x)=[x^4i(x)]\text{mod}(g(x))$ .

## A 2. DESCODIFICAÇÃO

### A 2.1 PRIMEIRO EXEMPLO DE DESCODIFICAÇÃO

Admitamos que o polinómio recebido tem 2 erros:

$$v(x) = c(x) + e(x) = (\alpha^4x^6 + \alpha^4x^4 + \alpha^3x^3 + \alpha^6x + \alpha^6) + (x + \alpha^5)$$

$$v(x) = \alpha^4x^6 + \alpha^4x^4 + \alpha^3x^3 + \alpha^2x + \alpha$$

- Calcule-se  $S_j = V_j = \sum_{i=0}^{N-1} \alpha^{ij} v_i, j=0,1,\dots,N-1$

$$S_0 = \alpha^4 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^6$$

$$S_1 = \alpha^4\alpha^6 + \alpha^4\alpha^4 + \alpha^3\alpha^3 + \alpha^2\alpha + \alpha = \alpha^6$$

$$S_2 = \alpha^4\alpha^{6.2} + \alpha^4\alpha^{4.2} + \alpha^3\alpha^{3.2} + \alpha^2\alpha^2 + \alpha = \alpha^3$$

$$S_3 = \alpha^4\alpha^{6.3} + \alpha^4\alpha^{4.3} + \alpha^3\alpha^{3.3} + \alpha^2\alpha^3 + \alpha = \alpha^2$$

$$S_4 = \alpha^4\alpha^{6.4} + \alpha^4\alpha^{4.4} + \alpha^3\alpha^{3.4} + \alpha^2\alpha^4 + \alpha = 1$$

$$S_5 = \alpha^4\alpha^{6.5} + \alpha^4\alpha^{4.5} + \alpha^3\alpha^{3.5} + \alpha^2\alpha^5 + \alpha = \alpha^3$$

$$S_6 = \alpha^4\alpha^{6.6} + \alpha^4\alpha^{4.6} + \alpha^3\alpha^{3.6} + \alpha^2\alpha^6 + \alpha = \alpha^5$$

Daqui resulta  $S(x) = \alpha^5x^6 + \alpha^3x^5 + x^4 + \alpha^2x^3 + \alpha^3x^2 + \alpha^6x + \alpha^6$ .

- Calcule-se o polinómio de localização de erros,  $\Lambda(x)$ , usando o algoritmo de Berlekamp-Massey, conforme está ilustrado na tabela seguinte:

Tabela A 3

r	$\Delta_r$	$\Lambda(x)=T(x)$	B(x)	L
0			1	0
1	$\alpha^6$	$\alpha^6x+1$	$\alpha$	1
2	$\alpha^2$	$\alpha^4x+1$	$\alpha x$	1
3	$\alpha^6$	$x^2+\alpha^4x+1$	$\alpha^5x+\alpha$	2
4	$\alpha^5$	$\alpha x^2+\alpha^3x+1$	$\alpha^5x^2+\alpha x$	2

- Verifique-se se o decodificador vai ser capaz de evitar uma falha na decodificação da palavra recebida. Para fazer este teste basta calcular

$$S_j = \sum_{i=1}^{L=2} \Lambda_i S_{j-i}, \quad j=5,6,\dots,11$$

verificando-se que  $S_{((7+j))}=S_j, \quad j=1,2,3,4.$

- Corrijam-se os síndromas de modo a obter o espectro do vector de erros:

Tabela A 4

r	$\Delta_r$	$E_r=S_r-\Delta_r$
5	$\alpha^3$	0
6	$\alpha^6$	$\alpha$
7	$\alpha^3$	$\alpha^4$

Então

$$E(x)=E_6x^6+E_5x^5+E_4x^4+E_3x^3+E_2x^2+E_1x+E_0=\alpha x^6+x^4+\alpha^2x^3+\alpha^3x^2+\alpha^6x+\alpha^4$$

com coeficientes  $E_0=E_7=S_7, E_6=S_6$  e  $E_5=S_5$  (Tabela A.4), e ainda, de acordo com os síndromas iniciais,  $E_1=S_1, E_2=S_2, E_3=S_3,$  e  $E_4=S_4.$

- Corrijam-se os síndromas de modo a obter o espectro da palavra de código:

$$C(x)=V(x)-E(x)=(\alpha^5x^6+\alpha^3x^5+x^4+\alpha^2x^3+\alpha^3x^2+\alpha^6x+\alpha^6)+(\alpha x^6+x^4+\alpha^2x^3+\alpha^3x^2+\alpha^6x+\alpha^4)$$

$$C(x)=\alpha^6x^6+\alpha^3x^5+\alpha^3$$

- Aplique-se a IDFT, para calcular os símbolos  $c_i = \sum_{j=0}^{N-1} \alpha^{-ij} C_j$ ,  $i=0,1,\dots,N-1$ , ou seja,

$$c_0 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 + \alpha^6 = \alpha^6$$

$$c_1 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5} + \alpha^6 \alpha^{-6} = \alpha^6$$

$$c_2 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5.2} + \alpha^6 \alpha^{-6.2} = 0$$

$$c_3 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5.3} + \alpha^6 \alpha^{-6.3} = \alpha^3$$

$$c_4 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5.4} + \alpha^6 \alpha^{-6.4} = \alpha^4$$

$$c_5 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5.5} + \alpha^6 \alpha^{-6.5} = 0$$

$$c_6 = \alpha^3 + 0 + 0 + 0 + 0 + \alpha^3 \alpha^{-5.6} + \alpha^6 \alpha^{-6.6} = \alpha^4$$

Daqui resulta que  $c(x) = \alpha^4 x^6 + \alpha^4 x^4 + \alpha^3 x^3 + \alpha^6 x + \alpha^6$ .

- Fazendo a descodificação sistemática, obtemos a palavra de informação  $i(x) = \alpha^6 x + \alpha^6$  sem erros, tal como se esperava.

## A 2.2 SEGUNDO EXEMPLO DE DESCODIFICAÇÃO

Admitamos que o polinómio recebido não tem erros e tem  $\rho=4$  rasuras nas quatro últimas posições, identificadas com o coeficiente 1:

$$v(x) = c(x) + e(x) + f(x) = \alpha^4 x^6 + \alpha^4 x^4 + x^3 + x^2 + x + 1$$

- Inicialize-se  $\Lambda(x) = B(x) = 1$  e  $L = r = 0$ .
- Calcule-se  $S_j = V_j = \sum_{i=N-1}^0 \alpha^{ij} v_i$  para  $j=0,1,\dots,N-1$ .

$$S_0 = \alpha^4 + \alpha^4 + 1 + 1 + 1 + 1 = 0$$

$$S_1 = \alpha^4 \alpha^6 + \alpha^4 \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^6$$

$$S_2 = \alpha^4 \alpha^{6.2} + \alpha^4 \alpha^{4.2} + \alpha^{3.2} + \alpha^{2.2} + \alpha^2 + 1 = \alpha^6$$

$$S_3 = \alpha^4 \alpha^{6.3} + \alpha^4 \alpha^{4.3} + \alpha^{3.3} + \alpha^{2.3} + \alpha^3 + 1 = \alpha^6$$

$$S_4 = \alpha^4 \alpha^{6.4} + \alpha^4 \alpha^{4.4} + \alpha^{3.4} + \alpha^{2.4} + \alpha^4 + 1 = \alpha^4$$

$$S_5 = \alpha^4 \alpha^{6.5} + \alpha^4 \alpha^{4.5} + \alpha^{3.5} + \alpha^{2.5} + \alpha^5 + 1 = 1$$

$$S_6 = \alpha^4 \alpha^{6.6} + \alpha^4 \alpha^{4.6} + \alpha^{3.6} + \alpha^{2.6} + \alpha^6 + 1 = \alpha^3$$

Daqui resulta  $S(x) = \alpha^3 x^6 + x^5 + \alpha^4 x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^6 x$

- Calcule-se o polinómio de localização de erros e rasuras,  $\Lambda(x)$ , para  $r=1, \dots, \rho=2t=4$ .

Tabela A 5

r	$B(x) = \Lambda(x) = \Lambda(x) - U_r x \Lambda(x)$
1	$x+1$
2	$\alpha x^2 + \alpha^3 x + 1$
3	$\alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x + 1$
4	$\alpha^6 x^4 + \alpha^5 x^3 + \alpha^5 x^2 + \alpha^2 x + 1$

- Verifique-se se o decodificador vai ser capaz de evitar uma falha na decodificação da palavra recebida, bastando para isso calcular

$$S_j = \sum_{i=1}^{L=4} \Lambda_i S_{j-i}, \quad j=5, 6, \dots, 11, \text{ constatando que } S_{((7+j))} = S_j, \quad j=1, 2, 3, 4.$$

- Corrijam-se os síndromas de modo a obter o espectro do vector de erros:

Tabela A 6

r	$\Delta_r$	$E_r = S_r - \Delta_r$
5	$\alpha^3$	$\alpha$
6	$\alpha^6$	$\alpha^4$
7	$\alpha^3$	$\alpha^3$

Então

$$\begin{aligned} C(x) &= V(x) - E(x) = \\ &= (\alpha^3 x^6 + \alpha^7 x^5 + \alpha^4 x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^6 x) + (\alpha^4 x^6 + \alpha x^5 + \alpha^4 x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^6 x + \alpha^3) \\ &= \alpha^6 x^6 + \alpha^3 x^5 + \alpha^3 \end{aligned}$$

tal como no exemplo A.2.1.

- Aplicando a IDFT e fazendo a decodificação sistemática obtemos de novo a palavra de informação  $i(x) = \alpha^6 x + \alpha^6$ .

### A 2.3 TERCEIRO EXEMPLO DE DESCODIFICAÇÃO

Consideremos uma situação em que há 2 erros  $e(x) = \alpha^3 x^2 + \alpha^5$  e uma rasura no penúltimo símbolo resultando então:

$$v(x) = c(x) + e(x) + f(x) = \alpha^4 x^6 + \alpha^4 x^4 + \alpha^3 x^3 + \alpha^3 x^2 + x + \alpha$$

- Inicialize-se  $\Lambda(x) = B(x) = 1$  e  $L = r = 0$ .
- Calcule-se a DFT da palavra recebida  $V_j$  sendo  $S_j = V_j = \sum_{i=0}^{N-1} \alpha^{ij} v_i$ ,  $j=0, 1, \dots, N-1$ .

$$S_0 = \alpha^4 + \alpha^4 + \alpha^3 + \alpha^3 + 1 + \alpha = \alpha^3$$

$$S_1 = \alpha^4 \alpha^6 + \alpha^4 \alpha^4 + \alpha^3 \alpha^3 + \alpha^3 \alpha^2 + \alpha + \alpha = \alpha^3$$

$$S_2 = \alpha^4 \alpha^{6 \cdot 2} + \alpha^4 \alpha^{4 \cdot 2} + \alpha^3 \alpha^{3 \cdot 2} + \alpha^3 \alpha^{2 \cdot 2} + \alpha^2 + \alpha = 0$$

$$S_3 = \alpha^4 \alpha^{6 \cdot 3} + \alpha^4 \alpha^{4 \cdot 3} + \alpha^3 \alpha^{3 \cdot 3} + \alpha^3 \alpha^{2 \cdot 3} + \alpha^3 + \alpha = \alpha^2$$

$$S_4 = \alpha^4 \alpha^{6 \cdot 4} + \alpha^4 \alpha^{4 \cdot 4} + \alpha^3 \alpha^{3 \cdot 4} + \alpha^3 \alpha^{2 \cdot 4} + \alpha^4 + \alpha = \alpha^2$$

$$S_5 = \alpha^4 \alpha^{6 \cdot 5} + \alpha^4 \alpha^{4 \cdot 5} + \alpha^3 \alpha^{3 \cdot 5} + \alpha^3 \alpha^{2 \cdot 5} + \alpha^5 + \alpha = 0$$

$$S_6 = \alpha^4 \alpha^{6 \cdot 6} + \alpha^4 \alpha^{4 \cdot 6} + \alpha^3 \alpha^{3 \cdot 6} + \alpha^3 \alpha^{2 \cdot 6} + \alpha^6 + \alpha = \alpha$$

Obtém-se assim  $S(x) = \alpha x^6 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha^3 x + \alpha^3$

- Inicialize-se  $\Lambda(x)$  para  $r = \rho = 1$  do seguinte modo:

Tabela A 7

r	$B(x) = \Lambda(x) = \Lambda(x) - U_r x \Lambda(x)$
1	$x + \alpha$

- Calcule-se  $\Lambda(x)$  para  $r = \rho + 1 = 2, \dots, 2t = 4$  resultando a tabela A 10.

Tabela A 8

r	$\Delta_r$	$\Lambda(x) = T(x)$	$B(x)$	L
2	$\alpha^4$	$\alpha^5 x^2 + \alpha^2 x + 1$	$\alpha^4 x + \alpha^3$	2
3	$\alpha^4$	$\alpha^6 x^2 + \alpha^6 x + 1$	$\alpha^4 x^2 + \alpha^3 x$	2
4	$\alpha^4$	$\alpha x^3 + \alpha^2 x^2 + \alpha^6 x + 1$	$\alpha^2 x^2 + \alpha^2 x + \alpha^3$	3

- Verifique-se que o decodificador não vai ser capaz de evitar uma falha na decodificação bastando para isso calcular

$$S_j = \sum_{i=1}^{L=3} \Lambda_i S_{j-i}, \quad j=5,6,\dots,11,$$

Efectivamente, não se constata que

$$S_{((7+j))} = S_j, \quad j=1,2,3,4.$$

Note-se que isto significa que o decodificador funciona aqui eficazmente em termos de detecção de erros.

- Podíamos tentar, contudo, uma decodificação completa usando recursivamente o algoritmo de Berlekamp-Massey para as iterações  $r > 2t$ .

Tabela A 9

r	$\Delta_r$	$E_r = S_r - \Delta_r$
5	$\alpha^2$	$\alpha^2$
6	$\alpha^6$	$\alpha^5$
7	0	$\alpha^3$

- Procedendo como anteriormente,

$$C(x) = V(x) - E(x) = (\alpha x^6 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha^3 x + \alpha^3) + (\alpha^5 x^6 + \alpha^2 x^5 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha^3 x + \alpha^3)$$

$$C(x) = \alpha^6 x^6 + \alpha^2 x^5$$

- Aplicando a IDFT obteríamos  $c(x) = \alpha^4 x^6 + x^5 + \alpha^4 x^3 + \alpha^5 x^2 + \alpha^5 x + 1$ .
- Forçar a decodificação completa conduzia-nos neste caso a um bloco de informação incorrecto,

$$\alpha^5 x + 1 \neq i(x) = \alpha^6 x + \alpha^6$$