**UNIVERSIDADE ABERTA**

Departamento de Ciências e Tecnologia
Mestrado em Estatística, Matemática e Computação

Área Cientifica: Estatística Computacional

# Delineamento Experimental em Blocos Incompletos: Estudo de Casos Particulares

Carla Susete Gonçalves Francisco

Lisboa 2014

**UNIVERSIDADE ABERTA**

Departamento de Ciências e Tecnologia

Mestrado em Estatística, Matemática e Computação

Área Científica: Estatística Computacional

**Carla Susete Gonçalves Francisco**

Dissertação apresentada à Universidade Aberta

para obtenção do grau de mestre em

Estatística, Matemática e Computação

**Orientadora:** Professora Doutora Teresa Paula Costa Azinheira Oliveira

**Co-Orientadora:** Professora Doutora Sandra Maria Bargão Saraiva Ferreira

Lisboa 2014

*Dedico este trabalho à minha mãe*
*e à memória do meu Pai*

## Agradecimentos

À Professora Doutora Teresa Oliveira, minha orientadora agradeço pelo apoio, pela paciência, pelo constante incentivo, pela disponibilidade em partilhar a sua vasta experiência e pelas proveitosas discussões científicas sem as quais não teria sido possível realizar este trabalho.

À Professora Doutora Sandra Maria Bargão Saraiva Ferreira, agradeço a disponibilidade demonstrada e a sua indispensável contribuição para a realização deste trabalho sem a qual o mesmo não teria sido possível.

Ao Professor Doutor Amílcar Manuel do Rosário Oliveira, pelo seu contagiante entusiasmo pela Matemática, que com as suas aulas me permitiu alargar os meus horizontes estatísticos e computacionais.

Aos professores da parte curricular do mestrado agradeço pela disponibilidade e pelo constante incentivo na realização de todos os trabalhos que nos foram propostos.

À minha mãe Irene Francisco, agradeço o seu apoio incondicional e dedicação ao longo dos dois anos de mestrado, pois sempre me apoiou quando mais necessitei.

A toda a minha família, em particular à minha irmã Cátia e ao Filipe pela motivação e apoio nos momentos mais complicados.

Aos DDs, o David e Daniel pela inspiração e sentido de esperança que trazem ao futuro.

Aos meus colegas e amigos agradeço o encorajamento e as sugestões, em especial ao Avelino e à Paula.

Gostaria assim de deixar uma palavra de profunda gratidão a todos aqueles que, de uma forma direta ou indireta, contribuíram para a realização deste trabalho.

A todos, o meu eterno agradecimento.

## Resumo

O Delineamento Experimental em Blocos Incompletos reveste-se de uma enorme importância uma vez que faz a ponte entre a matemática aplicada e as aplicações da estatística em áreas tão diversas como a agricultura, a medicina, a biometria, a criptografia, a genética, a indústria, as ciências da educação, entre muitas outras. Tem por objetivo principal a obtenção da maior quantidade de informação possível, a partir de uma pesquisa experimental. Para tal, procede-se a uma análise comparativa entre as diferentes variedades ou tratamentos por forma a se poderem controlar as fontes de variação aleatórias através da divisão das unidades experimentais em blocos.

Seguidamente, procede-se à síntese de cada um dos capítulos:

No primeiro capítulo deste trabalho é feita uma introdução ao delineamento experimental em blocos. É também exposta a motivação para a abordagem desta temática.

No segundo capítulo apresenta-se uma introdução histórica ao delineamento experimental em blocos. É também desenvolvido com algum detalhe o estudo dos planos em blocos incompletos equilibrados.

No terceiro capítulo procede-se à investigação de casos particulares, nomeadamente dos planos com blocos repetidos, planos com diferentes dimensões e planos com número de réplicas variável, passando de seguida à classificação em famílias dos planos com repetições (BIBDR) - Balanced Incomplete Block Designs with Repeated Blocks (Planos em Blocos Incompletos Equilibrados com Repetições). A construção dos (BIBD) - Balanced Incomplete Block Designs com Repetições (BIBDR) é abordada como um Plano Otimal que proporciona facilidade de aplicação prática e se reveste de importância sob o ponto de vista económico, (Foody, W. & Hedayat, A, 1977), (Hedayat, A. S. & Hwang, H. L. 1984). Foi desenvolvido um programa em Basic para obtenção da lista de parâmetros dos possíveis BIBDR, com dimensão de bloco sete, tendo em conta as condições necessárias de construção dos BIBDR sobre certas restrições. Os planos são classificados atendendo às três famílias de BIBDR, definidas em (Hedayat, A. S. & Hwang, H. L. 1984).

O capítulo quatro explora as ligações existentes entre desenho experimental, matrizes de Hadamard e o risco de perda de dados nos Códigos QR.

No capítulo cinco aprofunda-se o estudo dos Códigos QR, explorando diversas aplicações e apresentando exemplos práticos.

No capítulo seis expõe-se uma introdução ao *software* estatístico R (*Project for Statistical Computing*) e exemplos práticos desenvolvidos neste, tendo por base a temática do delineamento experimental com blocos.

O capítulo sete apresenta diversos trabalhos de investigação com abordagens recentes ao delineamento experimental em blocos. Estes trabalhos abrangem temáticas diversas como a medicina, criptografia, ensaios clínicos, Códigos QR entre outros. Neste capítulo, destaca-se um estudo sobre a doença de Parkinson no âmbito dos ensaios clínicos.

A aplicação prática presente no capítulo oito mostra a análise de fiabilidade inter-examinador inspirada nesse estudo. Nesta aplicação serão analisados seis neurologistas que examinam dez pacientes com Parkinson.

No capítulo nove são sintetizadas algumas considerações finais e apresentadas perspetivas de investigação futura.

**Palavras chave:** Delineamento Experimental, Blocos Incompletos, BIBD, BIBDR.

## Abstract

The Design of Experiments considering incomplete blocks is of great importance since it bridges the gap between Applied Mathematics and Applications of Statistics in diverse areas such as agriculture, medicine, biometrics, encryption, genetics, industry and science education, among many others.

The Design of Experiments or Experimental Design has the main objective of obtaining as much information as possible from an experimental study. A comparative analysis of the different varieties or treatments is made, in order to be able to control the random sources of variation by dividing the experimental units in blocks.

Subsequently, we will synthesize each one of the chapters:

In the first chapter of this paper an introduction to Experimental Design in blocks is presented. It is also exposed the motivation to address this issue.

The second chapter presents a historical introduction to Experimental Design in blocks. It is also approached the study of balanced incomplete block designs and respective characteristics.

In the third chapter a research of special cases is developed, such as designs with repeated blocks, designs with different dimensions and designs with different number of replicas, followed by the classification in families of BIB designs with repetitions. The construction of BIBD with Repetitions (BIBDR) is carried out using Optimal Designs which provide ease of practical application and is of great importance from the economical point of view, (Foody, W. & Hedayat, A. 1977), (Hedayat, A. S. & Hwang, H. L.1984). A program in BASIC language has been developed in order to obtain the list parameter of possible BIBDR with seven block size, taking into account certain restrictions. These designs are classified according to the three families of BIBDR defined in (Hedayat, A. S. & Hwang, H. L.1984).

Chapter four explores the links between Experimental Design, Hadamard matrices and the risk of data loss in QR Codes.

Chapter five deepens the study of QR Codes, exploring different applications and presenting practical examples.

Chapter six presents an introduction to statistical *software* R (Project for Statistical Computing) and practical examples developed in this, based on the theme of Experimental Design with blocks.

The seventh chapter presents recent approaches and applications of Experimental Design considering blocks. These works cover different topics such as medicine,

encryption, clinical tests, QR Codes and more. The approach of the previous section on clinical studies highlighted a study of Parkinson's disease.

Chapter eight shows a virtual practical application of this, in the analysis of an inter reliability inspired in this study. In this application a design considering six neurologists who examined ten patients with Parkinson's disease will be considered.

In chapter nine, some final remarks are summarized and perspectives for future research are presented.

**Key words:** Experimental Design, Incomplete Block, BIBD, BIBDR.

# Índice

# Lista de figuras

# Lista de tabelas

## Lista de abreviaturas e siglas

**ANOVA:** *Analysis of Variance* (Análise de Variância).

**ATM:** *Automated teller machine* (Máquina multibanco).

**IBD ou PBI:** *Incomplete Block Designs* (Planos em Blocos Incompletos).

**BIBD ou PBIE:** *Balanced Incomplete Block Designs* (Planos em Blocos Incompletos Equilibrados).

**BIBDR ou PBIER:** *Balanced Incomplete Block Designs with Repeated Blocks* (Planos em Blocos Incompletos Equilibrados com Repetições).

**CF:** Coeficiente de Fiabilidade.

$\boldsymbol{GF(q)}$**:** *Galois Field* (Campo Finito).

**MA ou AM**: Memetic algorithms (Algoritmo Memético).

**PBD:** *Pairwise Balanced Designs* (Planos Equilibrados Emparelhados).

**PBIBD:** *Partially Balanced Incomplete Block Designs* (Planos em Blocos Incompletos Parcialmente Equilibrados).

**QR Code:** Q*uick Response Code* (Códigos QR).

**RS Code:** *Reed-Solomon Code* (Código Reed-Solomon).

**SBIBD:** *Symmetric Balanced Incomplete Block Designs* **(**Planos em Blocos Incompletos Equilibrados Simétricos).

**SLE:** *Single Loss Expectancy* (Custo monetário expectável)

**TICs**: Tecnologias da informação e comunicação.

# Capítulo 1

# Introdução, motivação e objetivos

## 1.1 – Introdução

O delineamento em blocos encontra aplicação em todas as áreas da investigação humana, incluindo a Agricultura, Biologia, Engenharia, Medicina, Ciências Físico-Químicas e investigação Industrial. O mais primevo dos delineamentos por blocos é o delineamento inteiramente aleatório (Blocos Completos). No entanto, em muitas situações práticas, a adoção de um delineamento desse género não é adequado e em alguns casos, não é de todo viável. Este facto levou ao desenvolvimento de vários tipos de delineamento por Blocos Incompletos, que por sua vez têm sido amplamente utilizados para experiências em diversas áreas. Além disso estes delineamentos colocaram muitos problemas interessantes, porém desafiadores, à área da Matemática Combinatória.

As bases modernas do delineamento experimental foram estabelecidas por R.A. Fisher durante a primeira parte do século 20 e desde então, esta área tem tido um crescimento fenomenal.

O delineamento experimental tem sido, desde há muito, uma parte integrante de quase todas as investigações científicas e portanto desempenha um papel fundamental na prática da Estatística e da pesquisa científica.

A formação na área da Estatística sempre enfatizou o papel do delineamento experimental, fundamental na extração de informação correta e na obtenção de inferências válidas ao problema em estudo.

Ao projetar uma experiência, os princípios de aleatoriedade, replicação e controlo local, são de vital importância. Estes princípios foram inicialmente enunciados por Fisher, enquanto concretizava o planeamento de experiências agrícolas.

Foi observado por Fisher que a colocação, aleatoriamente, dos tratamentos nas unidades experimentais, elimina o viés na avaliação de diferenças entre tratamentos. Em determinadas situações experimentais podem existir variações sistemáticas presentes nas unidades experimentais.

Por exemplo, numa experiência num campo agrícola, as unidades experimentais consideradas são tipicamente parcelas de terra. Numa tal experiência, pode existir um gradiente de fertilidade, tal que parcelas com o mesmo nível de fertilidade são mais homogéneas que as que possuem um nível de fertilidade diferente. Em experiências com suínos, os quais se consideram unidades experimentais, é muito plausível que os suínos que pertencem à mesma ninhada estejam geneticamente mais próximos uns dos outros do que aqueles que pertencem a ninhadas diferentes. De forma similar, em experiências realizadas com gado, diversas raças podem estar envolvidas e espera-se que animais que pertencem à mesma raça sejam estatisticamente mais semelhantes do que os pertencentes a raças diferentes. No âmbito de ensaios clínicos com pacientes, estes formam as unidades experimentais. Os ensaios podem ser realizados em diferentes centros e pacientes do mesmo centro podem ser mais semelhantes do que de outros centros, devido a diferenças de práticas de tratamento ou procedimentos de gestão seguidos nos diferentes centros.

Nas situações dos exemplos anteriores a utilização de desenho experimental totalmente aleatório não é apropriado. De facto deve tirar-se partido da informação à priori acerca das variações sistemáticas, por forma a que esta informação possa ser utilizada para eliminar o efeito dessa variabilidade, o que se irá refletir num erro experimental mais reduzido, aumentando assim a precisão da experiência.

No delineamento de experiências em blocos casualizados, o número de parcelas por bloco deve corresponder ao número de tratamentos.

Utiliza-se um delineamento em Blocos Incompletos quando é impraticável utilizar todos os tratamentos em cada um dos blocos.

Nos delineamentos em Blocos Incompletos Equilibrados nenhuma variedade ocorre mais do que uma vez no mesmo bloco.

## 1.2 – Motivação e objetivos

Devido à vasta aplicação do delineamento experimental em Blocos Incompletos Equilibrados a áreas de vanguarda da investigação existem ainda muitas questões em aberto no âmbito teórico, estes planos revestem-se de particular interesse e justifica-se assim a importância do estudo dos mesmos nesta dissertação.

# Capítulo 2

# O aparecimento dos modelos avançados de planeamento de experiências

## 2.1 – Introdução Histórica

Frank Yates, de nacionalidade Britânica, nascido em 1902, desenvolveu uma apetência pela matemática ainda em tenra idade, tendo obtido por mérito uma bolsa de estudo universitária e concluído o curso com menções honrosas. Após ter passado dois anos a lecionar no ensino secundário, Yates decidiu que queria utilizar os seus dotes na área da matemática para fazer algo que tivesse uma aplicação mais prática, pelo que se tornou assessor do grupo "*Gold Coast Survey"*. Nesta fase Yates desenvolveu uma grande apreciação pelo método dos mínimos quadrados de Gauss, e pela régua de cálculo e outros auxiliares do mesmo género, que utilizava para desenvolver a aritmética de forma eficiente, precisa e bem organizada. Por mero acaso Yates conhece R. A. Fisher ficando selecionado para uma vaga da *Rothamsted Experimental Station*, uma das mais antigas instituições de pesquisa agrícola, da Inglaterra, Yates, F. (2005).

Quando Fisher foi nomeado para lecionar na *University College of London* Yates assume a chefia da Estatística na *Rothamsted Experimental Station* e acaba por ficar nesse posto até se reformar. Yates trabalhou em desenho experimental, na maioria das vezes em colaboração com Fisher. Em 1936 publica um trabalho sobre desenho experimental em blocos incompletos, que se provou muito importante para a realização de experiências biológicas. Com o aparecimento do computador, Yates torna-se um entusiástico utilizador destes, defendendo que para se ser um bom estatístico é necessário utilizar as melhores ajudas computacionais e assim, em 1954, comprou um computador para ajudar na análise estatística que efetuava em *Rothamsted*. Devido à sua velocidade, rigor e possibilidade de mecanização do trabalho anteriormente apenas realizável à mão, Yates sugeriu que estes seriam muito úteis para biólogos e que na estatística se conseguiriam realizar cálculos antes julgados impossíveis devido ao tempo que teria de ser despendido se estes tivessem de ser executados de maneira tradicional.

Por existirem poucos programas na sua época, Yates encorajava as pessoas a desenvolverem programas para resolverem problemas clássicos da Estatística. De forma visionária acrescenta que o código produzido deveria ser independente da máquina, por forma a ser executado em qualquer local, muito ao estilo da recente linguagem Java.

## 2.2 – Planos em Blocos Incompletos Equilibrados

Leonhard Paul Euler (1707-1783) Físico e Matemático suíço, foi quem iniciou o estudo dos Quadrados Latinos, para a resolução de complexos problemas de Matemática Combinatória.

Mais tarde, outros matemáticos como Yates em 1936 desenvolveram o seu estudo também em Matemática Combinatória mais exatamente nos BIBD - Planos de Blocos Equilibrados Incompletos (*Balanced Incomplete Block Designs*), tratando-se estes de uma particularidade dos IBD - Planos de Blocos Incompletos (*Incomplete Block Designs*).

(Cochran, W. G. & Cox, G. M. 1957) definem 3 tipos de blocos incompletos equilibrados:

Tipo I - Experiências em que os blocos possam ser agrupados em repetições;
Tipo II - Experiências em que os blocos possam ser dispostos em grupos de repetições;
Tipo III - Experiências cujos blocos não possam ser agrupados em repetições ou grupos de repetições.

(Oliveira, T. A., 1999) apresenta a seguinte definição:

*Os Planos em Blocos Incompletos Equilibrados são planos para v variedades em b blocos, em que cada bloco contém k parcelas, com* $k < v$ *. Cada variedade repete-se r vezes no total dos b blocos e cada par de variedades aparece junto nos diversos blocos* $\lambda$ *vezes. Nenhuma variedade ocorre mais do que uma vez no mesmo bloco.*

E também segundo (Oliveira, T. A., 1999), para os BIBD resolúveis, vem que:

*Quando é possível separar os b blocos em r conjuntos de m blocos cada, b = mr, de modo a que cada variedade ocorra apenas uma vez entre os blocos de um dado conjunto e cada conjunto forme uma réplica completa estamos perante um BIBD resolúvel.*

Os BIBD permitem a simplificação da análise dos resultados obtidos e das experiências. Yates definiu a seguinte restrição: cada par de tratamentos ocorre ao mesmo tempo em $\lambda$ blocos, nos quais $\lambda$ é uma constante.

Assim, o Plano de Blocos Equilibrados Incompletos é caracterizado por ser equirreplicado, apropriado e binário.

Considere-se uma experiência agrícola, em que se quer comparar o rendimento da produção de *v* variedades de grão. É bastante provável que exista uma interação entre as condições ambientais, tais como o tipo de solo, quantidade de precipitação, drenagem, etc. e a variedade do grão, o que vai influenciar na produção.

Então escolhem-se *b* blocos, que correspondem a conjuntos de parcelas de terreno onde se vai desenvolver a experiência. Estes blocos são escolhidos para que as condições ambientais sejam o mais uniforme possível em cada um dos blocos.

Noutros tipos de experiências onde o ambiente não seja um fator tão preponderante, os blocos podem ser distinguidos como sendo parcelas que recebem um tipo particular de tratamento, como por exemplo, um tipo específico de fertilizante. Desta forma a classificação de parcelas ou lotes de terreno experimental em blocos, e variedades, pode ser utilizada sempre que existem dois fatores que podem influenciar o rendimento da produção.

A técnica de plantar cada variedade num lote de terreno, em cada bloco, pode, para experiências de grande dimensão, tornar-se demasiado caro ou simplesmente impraticável. Para resolver esta problemática pode utilizar-se blocos mais pequenos que não contenham todas as variedades.

De modo a minimizar os efeitos do mero acaso devido aos blocos incompletos, pretende-se desenhar os blocos de modo a que probabilidade, de duas variedades a serem comparadas, seja a mesma para todos os pares. Esta propriedade é chamada de equilíbrio. Várias técnicas estatísticas e em particular a análise de variância - ANOVA, podem ser utilizadas para inferir conclusões acerca da experiência.

Na utilização corrente, faz-se referência a um desenho como sendo um par ordenado $(X, \beta)$, onde $X$ é um conjunto de elementos, chamados pontos e $\beta$ é uma coleção de sub-conjuntos de $X$, chamados blocos.

Um BIBD é portanto um conjunto $X$, descrito anteriormente, de $v \geq 2$ elementos, chamados variedades, ou tratamentos, e uma coleção de $b > 0$ subconjuntos de $X$, chamados blocos, por forma a que as seguintes condições sejam satisfeitas:

- Cada bloco consiste exatamente em $k$ variedades, com $v > k > 0$,
- Cada variedade aparece exatamente em $r$ blocos, com $r > 0$,
- Cada par de variedades aparece simultaneamente exatamente em $\lambda$ blocos, com $\lambda > 0$.

Se $\beta$ é um conjunto, quando $\lambda > 1$, então esse desenho diz-se do tipo simples, caso contrário, $\lambda \leq 1$, o desenho é de blocos repetidos.
Os BIBD são muitas vezes referidos como desenhos de cinco parâmetros não independentes, $v$ , $b$ , $r$ , $k$ e $\lambda$, sendo números inteiros, tal que :
$v$ representa o número de tratamentos ou variedades;

$b$ representa o número de blocos;

$r$ é o número de ocorrências de cada variedade;

$k$ o tamanho do bloco;

$\lambda$ o número de blocos onde cada par de variedades ocorre.

Um plano em blocos incompletos equilibrados pode ser construído tomando combinações de $v$, $k$ a $k$, e impondo uma determinada combinação das variedades em cada bloco, (Silva, P., 2009).

Um exemplo de um desenho com os parâmetros: (7,7,3,3,1) é dado pelo conjunto *X* o qual é constituído pelas variedades 1,2,3,4,5,6,7 e pelos blocos {1,2,4}, {2,3,5}, {3,4,6}, {4,5,7}, {5,6,1}, {6,7,2} e {7,1,3}. O tamanho de cada bloco, como se pode facilmente observar é 3 e o número de repetições é também 3. Cada par de variedades aparece em apenas um bloco, pelo que $\lambda = 1$.

Outro exemplo é um desenho com os parâmetros: (4,4,3,3,2), dado pelo conjunto *X*, constituído pelas variedades 1,2,3,4 e pelos blocos {1,2,3}, {2,3,4}, {3,4,1} e {4,1,2}.

Um exemplo um pouco maior é dado pelo desenho com os parâmetros: (8,14,7,4,3) dado pelo conjunto *X*, constituído pelas variedades 1,2,3,4,5,6,7,8 e pelos blocos {1,3,7,8},{1,2,4,8},{2,3,5,8},{3,4,6,8},{4,5,7,8},{1,5,6,8},{2,6,7,8},{1,2,3,6}, {1,2,5,7},{1,3,4,5},{1,4,6,7},{2,3,4,7} {2,4,5,6} e {3,5,6,7};

Existem algumas condições que os parâmetros de um BIBD têm de satisfazer. Essas condições são inferidas do seguinte teorema:

**Teorema** – Dado um desenho de parâmetros $v, b, r, k, \lambda$ , Então:

- $bk = vr$
- $r(k-1) = \lambda(v-1)$.

**Demonstração:** Considere-se o conjunto de pares $(X, \beta)$, onde *X* é uma variedade e $\beta$ é um bloco que contém *X*. Contando este conjunto de duas formas possíveis, chega-se à primeira equação.

Existem *v* possíveis valores para *X* e como cada um aparece em *r* blocos, $vr$ conta como sendo o número desses pares. Por outro lado, existem *b* blocos e cada um contém *k* variedades, assim sendo, *bk* também conta o número desses pares.

A segunda equação é também obtida através de contagem. Deixe-se fixa uma determinada variedade, que se designará por p e conte-se o número de pares de variedades, *{p, y}* onde *p* e *y* aparecem juntas em qualquer bloco.
Se o par aparece mais do que uma vez, então este será contado esse número de vezes.

Existem $v$-1 escolhas possíveis de *y* e cada um desses pares irá aparecer em $\lambda$ blocos em conjunto, pelo que existem $\lambda(v-1)$ pares.

Por outro lado, p aparece em r blocos e pode ser emparelhado com k-1 outros elementos, em qualquer desses blocos, logo tem-se que $r(k-1) = \lambda(v-1)$.

Os cinco parâmetros não são independentes. Tipicamente consideram-se b e r como dependentes, e assim faz-se referência a desenhos de experiências $v$, k, $\lambda$.

Dos resultados anteriores vem que: $r = \frac{\lambda(v-1)}{k-1}$ e $b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{k^2-k}$

**Corolário:**

Se existe um plano ($v$, k, $\lambda$), então $\lambda(v\text{-}1) \equiv 0 \bmod (k\text{-}1)$ e $\lambda v(v\text{-}1) \equiv 0 \bmod k(k\text{-}1)$

Dado um determinado plano ($v$, k, $\lambda$), este pode ser representado como sendo uma matriz $v \times b$, que se designa por matriz de incidência do plano. As linhas desta matriz são etiquetadas com as variedades do plano, e as colunas com os blocos. Coloca-se um "1" na célula (i, j) da matriz se a variedade i está contida no bloco j, caso contrário coloca-se um "0". Cada linha da matriz incidência tem *r* 1's, cada coluna tem *k* 1's e, cada par de linhas distinto tem $\lambda$ 1's em comum. Estas observações conduzem a uma útil matriz identidade.

**Exemplo:**

Para o desenho experimental {1,2,3}, {2,3,4}, {3,4,1}, {4,1,2} constrói-se a seguinte matriz de incidência (Tabela 1)

| | {1,2,3} | {2,3,4} | {3,4,1} | {4,1,2} |
|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 |
| 2 | 1 | 1 | 0 | 1 |
| 3 | 1 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 1 |

**Tabela 2** – Matriz de incidência de um BIBD.

Considere-se o seguinte teorema sobre a matriz identidade para planos em blocos:

**Teorema** - seja A uma matriz {0,1}, $v \times$ b. Esta é matriz de incidência do plano $(v, k, \lambda)$, se e só se $AA^T = (r-\lambda)I + \lambda J$ e $u_a A = ku_b$ , onde I é a matriz identidade $v \times v$, J é a matriz $v \times v$, de todos os 1's e $u_a$ é um vetor composto por 1's, de comprimento a.

**Prova do teorema** – No produto, uma entrada fora da diagonal é o produto interno entre duas linhas distintas de A, que tem de ser $\lambda$.

Uma entrada na diagonal é o produto interno de uma linha de A com ela própria, e por isso é igual a *r*. A segunda condição diz que a soma de cada coluna de A é igual a *k*.

Por outro lado, considere-se $(X, \beta)$ como sendo o plano com matriz de incidência A.

Claramente dizer que $|X| = v$, $|\beta| = b$, e que cada bloco tem *k* elementos, resulta de $u_a A = ku_b$.

Da expressão para $AA^T$ obtém-se que cada elemento está contido em *r* blocos, e que, cada par de elementos distintos, está contido em $\lambda$ blocos. Por conseguinte, $(X, \beta)$ é um plano $(v, k, \lambda)$. Sem esta última condição não seria possível provar que os blocos têm todos o mesmo tamanho. Se se ignorar essa restrição, a mesma prova da demonstração do teorema fica equivalente a um tipo de desenho mais genérico, que são os PBD (*Pairwise Balanced Designs*) ou Planos Equilibrados, dois a dois.

Um PBD é um desenho $(X, \beta)$, onde, cada par de pontos distinto, está contido em exactamente $\lambda$ blocos. Um PBD é regular se cada ponto aparece em exatamente r blocos. Um PBD sem nenhum bloco igual a *X* é um PBD próprio, enquanto um PBD com todos os blocos iguais a *X* é um PBD trivial. Os PBD podem ser ou não uniformes, caso o sejam, todos os blocos têm o mesmo tamanho.

Se um BIBD tem parâmetros $k = 2$ e $\lambda = 1$, então é fácil verificar que:

$$r = v - 1 \text{ e } b = v(v - 1) / 2.$$

Isto significa que os blocos do plano são apenas todos os possíveis pares de variedades, isto é, o conjunto de blocos é o conjunto de todos os 2 - subconjuntos de $X$. Se as variedades forem interpretadas como sendo vértices e os blocos como sendo arestas, então um plano com estes parâmetros é um grafo completo com v vértices.

Do ponto de vista da teoria do desenho de experiências, estes planos não se mostram particularmente interessantes, embora sejam uma classe importante de grafos.

Considere-se o seguinte teorema acerca da desigualdade de Fisher:

**Teorema –** num plano $(v, k, \lambda)$ tem-se $b \geq v$.

**Prova do teorema –** Seja $b < v$ e seja A a matriz incidência do plano. Podem-se adicionar $v - b$ colunas de 0's a A para obter a matriz B do tipo $v \times v$.

Como essas colunas extra com 0's não vão alterar o cálculo dos produtos internos, tem de se ter $AA^T = BB^T$.

Calculando os determinantes obtém-se $\det(AA^T) = \det(BB^T) = \det(B).\det(B^T) = 0$ pois $\det(B) = 0$ devido às colunas com 0's. Assim, pela matriz identidade obtém-se:

$$\det(AA^T) = det\begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{pmatrix}.$$

Este determinante pode ser calculado subtraindo a primeira coluna a cada uma das outras colunas e em seguida adicionando cada linha à primeira linha, obtendo-se assim:

$$\det(AA^T) = det\begin{pmatrix} r + \lambda(v-1) & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{pmatrix}.$$

Assim, tem-se que:

$$\det(AA^T) = [r + \lambda(v-1)](r - \lambda)^{v-1}.$$

Mas, como $r, v$ e $\lambda$ são todos positivos, $r + \lambda(v-1) > 0$ , e como $k < 0$ tem-se que $r > \lambda$, logo este produto, no segundo termo, não pode ser zero, o que equivale a uma contradição.

Este resultado pode ainda ser obtido a partir de outra demonstração do teorema:

Seja A a matriz de incidência de um BIBD, e seja $s_j$ a linha número j de $A^T$. Note-se que $s_j$'s são todos vetores em $IR^v$ e existem b destes vetores.

Seja S o subconjunto $< s_j | 1 \leq j \leq b >$ , ou seja, todas as combinações lineares possíveis, em IR, dos $s_j$'s. Se se puder mostrar que S = $IR^v$, então, como um subconjunto de um espaço vetorial não pode ser mais pequeno do que uma base, tem que se ter $b \geq v$, e assim obtém-se o resultado pretendido.

Pode-se provar que S é um subconjunto de um espaço vetorial ao mostrar que todos os elementos da base, $e_i$ , estão contidos em S.

Observe-se que:

$$\sum_{j=1}^{b} s_j = (r, \dots, r),$$

logo,

$$\sum_{j=1}^{b} \frac{1}{r} s_j = (1, \dots 1).$$

Para um $i$ constante, se forem somadas apenas as linhas $s_j$ que têm um 1, na coluna número $i$ da matriz $A^T$, vem:

$$\sum s_j = (r-\lambda)e_i + (\lambda, \dots, \lambda) = (r-\lambda)e_i + \sum_{j=1}^{b} \frac{\lambda}{r} s_j.$$

Como $\lambda(v-1) = r(k-1)$ e $v > k$, segue que $r > \lambda$ e por isso $r - \lambda > 0$, resolvendo a equação em ordem a $e_i$ fica:

$$e_i = \sum \frac{1}{r-\lambda} s_j - \sum_{j=1}^{b} \frac{\lambda}{r(r-\lambda)} s_j.$$

Assim, para todos os $i$, $e_i$ é uma combinação linear dos $s_j$'s, logo está contido em S.

A desigualdade de Fisher é também válida para PBD's

É possível obter novos BIBDs a partir de outros já existentes.

O seguinte teorema explora uma forma de obter um BIBD a partir de outro, através da operação soma:

**Teorema –** Supondo que existe um BIBD $(v, k, \lambda_1)$ e um BIBD $(v, k, \lambda_2)$, então existe um BIBD $(v, k, \lambda_1+\lambda_2)$.

Do teorema anterior depreende-se que, supondo que existe um BIBD $(v, k, \lambda)$, então existe também um BIBD $(v, k, s\lambda)$ para todos os inteiros positivos.

Uma outra forma de construir um BIBD a partir de outro existente é utilizar a complementaridade de blocos, de acordo com o seguinte teorema:

**Teorema** – Se existe um BIBD $(v, b, r, k, \lambda)$, com $k \leq v - 2$, então existe um outro BIBD $(v, b, b - r, v - k, b - 2r + \lambda)$.

Num plano apesar das condições de equilíbrio de um BIBD não serem verificadas, pode acontecer, mesmo que se verifiquem condições parciais de equilíbrio.

(Mascarenhas, V. 2008) apresenta a seguinte definição de PBIBD:

**Definição**:

*Um esquema de associação com m classes, definido pelos respetivos parâmetros, é um Plano em Blocos Incompleto Parcialmente Equilibrado com m classes de associação (PBIBD (m)) se os $v$ tratamentos estão dispostos em b blocos de dimensão k e $k < v$, tal que:*

- *Cada tratamento ocorre no máximo uma única vez em cada bloco (plano binário) de dimensão k (plano próprio);*
- *Cada tratamento ocorre em $r$ blocos (plano equirreplicado);*
- *Dois tratamentos $\alpha$ e $\beta$ i-ésimos associados ocorrem juntos em $\lambda_i$ blocos, sendo $\lambda_i$ independente do par de tratamentos i-ésimos associados escolhidos.*

*Um PBIBD é definido pelos parâmetros $(v, b, r, k, \lambda_i)$ com $i = 1, 2, \ldots m$.*

# Capítulo 3

# Investigação de casos particulares

## 3.1 – Planos com blocos repetidos

O estudo dos Planos em Blocos Incompletos Equilibrados com Repetição de blocos (BIBDR) reveste-se de especial importância, pois estes encontram aplicações em áreas diversas como por exemplo na agricultura, na biologia, na investigação genética, na indústria em geral, na criptografia, na medicina, entre muitas outras.

Existe a necessidade de construção de Planos com Blocos Repetidos, não apenas por estar provado serem Planos Otimais, mas também do ponto de vista económico e da facilidade de aplicação prática em controlo de amostras e desenho de experiências. (Foody, W. & Hedayat, A., 1977), (Hedayat, A. S. & Hwang, H. L. 1984).

O método de compensação ou "*Trade-off*", apresentado por (Hedayat, A. & Li Shuo-Yen, R., 1979), foi o primeiro método proposto para a construção de BIBDR, sendo considerado um dos mais importantes. Se existem menos do que $b$ blocos distintos num BIB com $b$ blocos, então diz-se que o desenho tem blocos repetidos. Ao conjunto dos blocos distintos do desenho chama-se o suporte do desenho.

A construção de um BIB ($v, b, r, k, \lambda$) com blocos repetidos torna-se complicada sempre que os parâmetros b, r, e λ são primos entre si. Utiliza-se a notação BIBD (n, b, r, k, l| b*) para denotar um BIBD (n, b, r, k, l) com, precisamente, b* blocos distintos.

### Condições necessárias de existência dos BIBD com blocos repetidos

As condições necessárias de existência dos BIBD para se obter um limite para o número de blocos, de modo a que o plano admita a repetição de blocos, são apresentadas por (Sousa, M. F. & Oliveira, T. A., 2004).

As condições necessárias para existência dos BIBD (ou PBIE) são:

- $n = rv = bk$
- $r(k-1) = \lambda(v-1)$
- $b \geq v$ (Desigualdade de Fisher).

(Oliveira, T. A., 1999) demonstrou que se tem:

$$b \geq \frac{(k-1)(k-2)}{2} + 1 + k(r-1) - k\frac{k(k-1)(\lambda-1)}{2}.$$

Com base nas condições de existência dos PBIE, é desenvolvida em Oliveira, T. A. (1999) a análise dos casos $k = 3$, $k = 4$ *e* $k = 5$. O caso $k = 6$ é apresentado por (Oliveira, T. A., 2010b).

(Garcia, V. A., 2011) apresenta vários detalhes do estudo dos Planos em Blocos Incompletos Equilibrados com Repetições.

### 3.2 – Planos com blocos de diferentes dimensões

(Pearce, S. C., 1964) mostra duas formas sob as quais os Planos em Blocos Incompletos com diferentes dimensões ocorrem. Nalgumas experiências na qual é utilizado material biológico, nem sempre é possível ao investigador controlar o número de parcelas que podem ser agrupadas em blocos, como acontece com o número de animais obedecendo a certas condições. No entanto, pode acontecer também que, apesar de determinada experiência ter sido planeada para blocos de igual dimensão, no decorrer da mesma algum acidente se verifique e que faça com que a informação de algumas das parcelas seja invalidada. Apesar de este não ser o procedimento mais razoável a ter em consideração, nestas situações pode-se optar por considerar apenas os blocos com a mesma dimensão eliminando todos os excedentes, reduzindo desta forma a dimensão da amostra. Note-se porém que, caso não se verifique a homocedasticidade da variância do erro para todos os blocos, as conclusões obtidas podem ser questionadas.

Uma vez que a variância aumenta com a dimensão do bloco, já que depende da variabilidade das unidades experimentais dentro dos blocos, torna-se fulcral que sejam adotados planos com blocos de pequena dimensão conduzindo à redução do erro experimental. O pressuposto da homocedasticidade pode ser assumido para muitos casos, uma vez que não se verifica uma grande diferença na dimensão dos blocos. Podem ainda ser utilizados valores estimados para as observações omissas.

### 3.3 – BIBDR: Classificação em famílias e alguns exemplos

Este ponto do trabalho é dedicado ao estudo dos Planos em Blocos Incompletos Equilibrados com Repetição de Blocos, denotados de agora em diante por PIER.

A questão da existência de PIER para determinados valores de $v$, $b$, e $k$ tem vindo a interessar bastante os investigadores.

(Hedayat & Li Shu-Yen, R. 1979), apresentam o método de compensação ou "*Trade-off*", que permite a construção de PIER com vários tamanhos de suporte (um desenho experimental com blocos incompletos equilibrados com $b$ blocos, tem o tamanho de suporte $b^*$ quando exactamente $b^*$ da totalidade dos $b$ blocos, são distintos).

(Oliveira, T. A., 1994) apresenta vários detalhes do estudo deste método.

O método de "*Trade-off*" foi concebido para estudar planos com $v$ tratamentos arbitrários, dispostos em blocos de dimensão $k = 3$ em geral, e com $v = 7$ e $k = 3$ em particular, sendo posteriormente utilizados para construir e classificar em famílias os planos com blocos repetidos.

Para proceder a estudos mais detalhados das características destes planos é útil a divisão da coleção de todos os PBIE com $\lambda \geq 2$ em três famílias mutuamente exclusivas e exaustivas, de acordo com (Hedayat, A. S. & Hwang, H. L., 1984). Esta questão foi abordada em (Oliveira, T. A., 1994), bem como um estudo acerca dos PIER e das suas condições de existência.

(Hedayat, A. & Hwang, H. L., 1984) dividem os PBIE com $\lambda \geq 2$ em três famílias mutualmente exclusivas e exaustivas. O objetivo da divisão em famílias dos PBIE é simplificar o estudo dos planos com blocos repetidos.

Assim, temos:

- **Família 1:**
  Pertencem a esta família os PBIE *($v$ , $b$, $r$, $k$, $\lambda$)* cujos parâmetros $b$, $r$, $\lambda$ têm um divisor inteiro comum, $t$, com $t > 1$, e existe um ou mais PBIE do tipo PBIE*($v$,$b/t$,$r/t$,$k$,$\lambda/t$).*

- **Família 2:**

  Pertencem a esta família os PBIE ($v$, *b, r, k,* $\lambda$*)* cujos parâmetros *b, r,* $\lambda$ admitem um ou mais divisores inteiros comuns superiores à unidade, mas não existe o PBIE (*v,b/t,r/t,k,*$\lambda$*/t)* se $t > 1$ for um dos divisores comuns a *b,r,*$\lambda$.
  Reveste-se de especial importância testar as condições de existência de blocos repetidos.

- **Família 3 :**

  Os PBIE que pertencem a esta família são aqueles em que o maior divisor comum entre *b, r,* $\lambda$ é a unidade, ou seja *b, r,* $\lambda$ são números primos entre si.

A seguir serão apresentados os parâmetros para possíveis BIBDR para o caso particular em que $K = 7$, considerando: $5 \leq v \leq 50$, $b \leq 200$ e $\lambda \leq 10$.

Para construir a tabela de parâmetros dos planos em blocos incompletos equilibrados, com repetições (PIER) em que $K = 7$, torna-se necessário avaliar a desigualdade:

$$b \geq \frac{(7-1)(7-2)}{2} + 1 + 7(r-1) - \frac{7(7-1)(\lambda-1)}{2} <=>$$

$$<=> \ b \geq 7.r - 21.\lambda + 30 \ <=>$$

$$<=> \ b \geq 30 + 7(r - 3\lambda)$$

Pode-se traduzir esta expressão apenas em ordem a $r$ e a $\lambda$ , pois $rv = bk <=> b = \frac{rv}{k}$ e como $k = 7$ então $b = \frac{rv}{7}$ .

Assim, $\frac{rv}{7} \geq 30 + 7(r - 3\lambda) <=> rv \geq 210 + 49(r - 3\lambda)$ e como $r(k-1) = \lambda(v-1) <=> r = \frac{\lambda(v-1)}{k-1}$, que para $k = 7$, virá $r = \frac{\lambda(v-1)}{6}$.

Substituindo na expressão para *b*, temos:

$$\frac{\lambda(v-1)}{6} v \geq 210 + 49(\frac{\lambda(v-1)}{6} - 3\lambda) <=>$$

$$<=> \lambda v(v-1) \geq 1260 + 49\lambda(v-1) - 882\lambda <=>$$

$$<=> \lambda v^2 - \lambda v - 49\lambda v + 49\lambda + 882\lambda \geq 1260 <=>$$

$$<=> \lambda v^2 - 50\lambda v + 931\lambda \geq 1260 <=>$$

$$<=> \lambda(v^2 - 50v + 931) \geq 1260 <=>$$

$$<=> \lambda[(v-25)^2 + 306] \geq 1260$$

Para *K = 7*

$\lambda[(v-25)^2+306] \geq 1260.$

Tendo em atenção o comportamento da desigualdade $\lambda[(v-25)^2+306] \geq 1260$, e para $2 \leq \lambda \leq 10$, podemos deduzir o seguinte:

1) Para $\lambda = 2$ obtém-se:

$$(v-25)^2+306 \geq \frac{1260}{2} <=> (v-25)^2 \geq 324.$$

Para $v = 5$ a desigualdade verifica-se;

Para $v = 6$ a desigualdade verifica-se;

Para $v = 7$ a desigualdade verifica-se;

Para $8 \leq v \leq 42$ a desigualdade não se verifica;

Para $v \geq 43$ a desigualdade verifica-se.

2) Para $\lambda = 3$ obtém-se:

$$(v-25)^2+306 \geq \frac{1260}{3} <=> (v-25)^2 \geq 114.$$

Para $5 \leq v \leq 14$ a desigualdade verifica-se;

Para $15 \leq v \leq 35$ a desigualdade não se verifica;

Para $v \geq 36$ a desigualdade verifica-se;

3) Para $\lambda = 4$ obtém-se:

$$(v-25)^2+306 \geq \frac{1260}{4} <=> (v-25)^2 \geq 9.$$

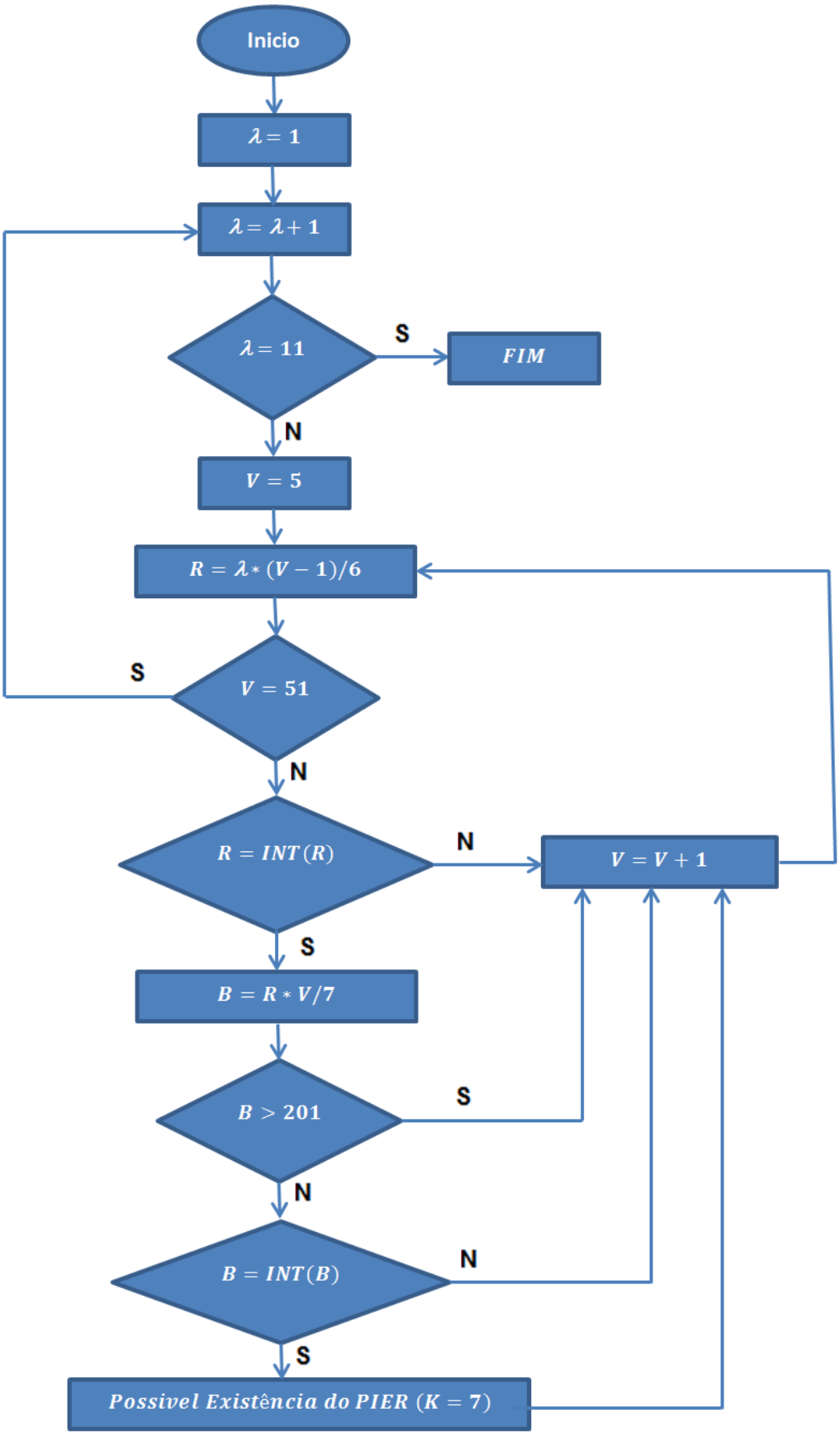
Para $6 \leq v \leq 22$ a desigualdade verifica-se;

Para $23 \leq v \leq 27$ a desigualdade não se verifica;

Para $v \geq 28$ a desigualdade verifica-se.

4) Para $5 \leq \lambda \leq 10$ é possível a existência de planos com blocos repetidos desde que $v \geq 5$.

### 3.4 – Fluxograma da rotina de classificação (*k=7*)



### 3.5 – Tabela de classificação por famílias

Na Tabela 2 é feita a Classificação por famílias de possíveis BIBDR com k = 7 .

| $v$ | $b$ | $r$ | $k$ | $\lambda$ | **Divisores de $b$ , $r$ , $\lambda$** | **Família** |
|---|---|---|---|---|---|---|
| 7 | 7 | 7 | 7 | 7 | 1,7 | 2 |
| | 8 | 8 | 7 | 8 | 1,2,4,8 | 2 |
| | 9 | 9 | 7 | 9 | 1,3,9 | 2 |
| | 10 | 10 | 7 | 10 | 1,2,5,10 | 2 |
| 8 | 8 | 7 | 7 | 6 | 1 | 3 |
| 13 | 26 | 14 | 7 | 7 | 1 | 3 |
| 14 | 26 | 13 | 7 | 6 | 1 | 3 |
| 15 | 30 | 14 | 7 | 6 | 1,2 | 1 |
| | 45 | 21 | 7 | 9 | 1,3 | 1 |
| 19 | 57 | 21 | 7 | 7 | 1 | 3 |
| 21 | 60 | 20 | 7 | 6 | 1,2 | 2 |
| | 90 | 30 | 7 | 9 | 1,3 | 2 |
| 22 | 44 | 14 | 7 | 4 | 1,2 | 2 |
| | 66 | 21 | 7 | 6 | 1,3 | 2 |
| | 88 | 28 | 7 | 8 | 1,2,4 | 2 |
| | 110 | 35 | 7 | 10 | 1,5 | 2 |
| 25 | 100 | 28 | 7 | 7 | 1 | 3 |
| 28 | 72 | 18 | 7 | 4 | 1,2 | 1 |
| | 108 | 27 | 7 | 6 | 1,3 | 1 |
| | 144 | 36 | 7 | 8 | 1,2,4 | 1 |
| | 180 | 45 | 7 | 10 | 1,5 | 1 |
| 29 | 116 | 28 | 7 | 6 | 1,2 | 1 |
| | 174 | 42 | 7 | 9 | 1,3 | 1 |
| 31 | 155 | 35 | 7 | 7 | 1 | 3 |
| 35 | 170 | 34 | 7 | 6 | 1,2 | 1 |
| 36 | 180 | 35 | 7 | 6 | 1 | 3 |
| 43 | 86 | 14 | 7 | 2 | 1,2 | 1 |
| | 129 | 21 | 7 | 3 | 1,3 | 1 |
| | 172 | 28 | 7 | 4 | 1,2,4 | 1 |
| 49 | 112 | 16 | 7 | 2 | 1,2 | 1 |
| | 168 | 24 | 7 | 3 | 1,3 | 1 |

**Tabela 3** – Classificação por famílias de possíveis BIBDR com $k = 7$ .

### 3.6 – Listagem do código fonte do programa em BASIC utilizado para obter os PIER para *k = 7*

```
10 LPRINT "O programa aceita K=7"
15 INPUT "K=";K
20 IF K=7 THEN GOTO 1000
50 LPRINT "Por favor escolha K=7"
60 STOP
1000 L=1
1002 L=L+1
1004 IF L=11 THEN GOTO 5000
1018 V=5
1040 R=L*(V-1)/6
1050 IF V=51 THEN GOTO 1002
1060 IF R=INT(R) THEN GOTO 1500
1080 V=V+1
1081 IF L=2 AND V>7 AND V<43 THEN GOTO 1080
1082 IF L=3 AND V>=15 AND V<=35 THEN GOTO 1080
1083 IF L=4 AND V>=23 AND V<=27 THEN GOTO 1080
1090 GOTO 1040
1500 B=R*V/7
1505 IF B > 201 THEN GOTO 1530
1510 IF B=INT(B) AND R*V=B*K AND R*(K-1)=L*(V-1) AND B>=V
THEN GOTO 1600
1530 V=V+1
1531 IF L=2 AND V>7 AND V<43 THEN GOTO 1530
1532 IF L=3 AND V>=15 AND V<=35 THEN GOTO 1530
1533 IF L=4 AND V>=23 AND V<=27 THEN GOTO 1530
1540 GOTO 1040
1600 LPRINT "Possível existência do PIER(" ;V;",";B;",";R;",";K;",";L;")"
1610 V=V+1
1611 IF L=2 AND V>7 AND V<43 THEN GOTO 1610
1612 IF L=3 AND V>=15 AND V<=35 THEN GOTO 1610
1613 IF L=4 AND V>=23 AND V<=27 THEN GOTO 1610
1620 GOTO 1040
5000 END
```

# Capítulo 4

# Explorando ligações entre Delineamento Experimental, matrizes de Hadamard e o risco de perda de dados nos Códigos QR

## 4.1 – Introdução

Jacques Salomon Hadamard foi um matemático francês que, durante a sua vida publicou incansavelmente artigos e livros de alta qualidade. Uma das obras pela qual ele é lembrado são as matrizes de Hadamard.

Os fundamentos do delineamento experimental por blocos foram estabelecidos por Sir. Ronald Fisher no início dos anos 30. Tornou-se uma das maiores áreas de desenvolvimento para a pesquisa em vários campos desde a agricultura até à medicina, bem como para outras áreas de pesquisa. Depois do seu trabalho inicial, várias técnicas foram apresentadas, com o objetivo de analisar os dados e apresentar novos tipos de delineamentos experimentais.

A pesquisa sobre Blocos Incompletos Equilibrados (*BIBD*) fez surgir vários problemas interessantes e desafiadores, dentro da matemática combinatória.

As matrizes de Hadamard estão presentes na nossa vida diária e é fácil e comum encontrar as suas diferentes aplicações baseadas nas novas tecnologias e códigos com base em imagens, como é o caso dos códigos de resposta rápida (Códigos QR).

Os Códigos QR são códigos de barras bidimensionais que podem ser facilmente lidos por dispositivos comuns que têm a função de captação de imagem, tal como é o caso dos *smartphones* (telemóveis).

A utilização de tais códigos é muito popular hoje em dia, em coisas simples tal como enviar uma mensagem de texto, uma imagem ou um endereço para uma página *Web* (hiperligação).

## 4.2 – Matrizes de Hadamard

Uma matriz de Hadamard é uma matriz quadrada $\boldsymbol{H_n}$ de ordem $n$ com elementos $\pm 1$ se $\boldsymbol{H_n H_n^T} \equiv n\boldsymbol{I_n}$. Se $\boldsymbol{H_n}$ é uma matriz de Hadamard então $\boldsymbol{H_n H_n^T} \equiv n\boldsymbol{I_n}$. Se qualquer linha ou coluna for multiplicada por $-1$ a matriz permanece de Hadamard.

Tomando isto em consideração, pode sempre escrever-se uma matriz de Hadamard tendo a primeira linha e primeira coluna apenas $+1$'s isto chama-se a forma usual de uma matriz de Hadamard.

Se $\boldsymbol{H_n}$ existe para $n \equiv 1$ então $\boldsymbol{H_2}$ pode ser escrita como:

$$\boldsymbol{H_2} \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

A condição necessária à existência de uma matriz de Hadamard $\boldsymbol{H_n}$, para $n > 2$ , é que $n \equiv 0 (mod\ 4)$; mais desenvolvimentos sobre estas matrizes poderão ser encontrados em (Marshall Hall, Jr., 1986).

Ainda se desconhece se esta condição necessária é suficiente. Matrizes de Hadamard para todos os valores permitidos de $n \leq 100$, com a excepção de $n \equiv 92$ já foram criadas, (Plackett, R. L. & J. P. Burman, 1946).

Os autores (Baumert, L.; Golomb, S. W. & Marshall Hall, Jr., 1962), descobriram uma matriz de Hadamard de ordem 92.

Matrizes de Hadamard para valores de $n < 424$ têm a sua existência confirmada. Se $\boldsymbol{H_m}$ e $\boldsymbol{H_n}$ são matrizes de Hadamard de ordem $m$ e $n$, respectivamente, então o seu produto tensor $H_m \otimes H_n$ é uma matriz de Hadamard de ordem $m \times n$.

Em particular, uma matriz de Hadamard $\boldsymbol{H_n}$ de ordem $n$, onde $n \equiv 2s$ e $s \geq 2$ é um número inteiro, pode ser construida fazendo o produto tensor de ordem $s$ de $\boldsymbol{H_2}$ por si mesma, tal como neste exemplo:

$$H_{2^s} \equiv \underbrace{H_2 \otimes H_2 \otimes \ldots \otimes H_2}_{s \text{ vezes}}$$

(Wallis, J., 1970) expõe várias propriedades das matrizes de Hadamard:

- Cada elemento é: $\pm 1$;
- O produto escalar de quaisquer dois vetores de linha distintos é zero;
- Uma matriz de Hadamard de ordem $4n$ tem como determinante $\pm(4n)^{2n}$;
- Se $H$ é uma matriz de Hadamard de ordem $4n$ então $H$ satisfaz a condição: $HH^T = 4nI_{4n}$;
- As matrizes de Hadamard podem ser transformadas noutras matrizes de Hadamard, permutando as linhas com as colunas e também através da multiplicação das linhas e colunas por $-1$. As matrizes que podem ser obtidas umas das outras, através destes métodos, dizem-se H-equivalentes. Nem todas as matrizes de Hadamard da mesma ordem são H-equivalentes;
- Todas as matrizes de Hadamard são H-equivalentes a uma matriz de Hadamard que tem todos os elementos na sua primeira linha e coluna iguais a $+1$. Matrizes nesta forma dizem-se normalizadas;
- Se $H$ é uma matriz de Hadamard normalizada, de ordem $4n$, então todas as linhas, excepto a primeira, possuem $2n, -1's$ e $2n, +1's$, e adicionalmente $n, -1's$ em qualquer linha sobreposta com $n, -1's$ existentes em cada outra linha;
- A ordem de uma matriz de Hadamard é 2 ou $4n$, com $n$ inteiro.

## 4.3 – Construção de Paley das Matrizes de Hadamard

A construção de Paley é um método para construir matrizes de Hadamard utilizando campos finitos. A construção foi descrita em 1933 pelo matemático Inglês, Raymond Paley. Utiliza resíduos quadráticos num campo finito $GF(q)$ onde $q$ é uma potência de um número primo ímpar. Existem duas versões da construção que dependem de $q$ ser coerente a 1 ou 3 (mod 4).

Se $q$ é coerente a 3 (mod 4) então:

$$\boldsymbol{H} \equiv \boldsymbol{I} + \begin{bmatrix} 0 & j^T \\ -j & Q \end{bmatrix}$$

é uma matriz de Hadamard de ordem $(q + 1)$. Aqui $\boldsymbol{j}$ é o vector de colunas só de 1's, de comprimento $q$ e $\boldsymbol{I}$ é a matriz identidade $(q + 1) \times (q + 1)$.

Se $q$ é coerente a 1 mod 4 então a matriz é obtida substituindo todas as entradas 0 em,

$$\begin{bmatrix} 0 & j^T \\ -j & Q \end{bmatrix}$$

pela matriz,

$$\begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$$

e todos os elementos $\pm$ 1 pela matriz,

$$\pm \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

é uma matriz de Hadamard de ordem $2(q + 1)$. Esta é uma matriz simétrica.

### 4.4 – A conjetura de Hadamard

A ordem de uma matriz de Hadamard tem de ser 1, 2, ou um múltiplo de 4. O produto de Kronecker entre duas matrizes de Hadamard de ordens $m$ e $n$ é uma matriz de Hadamard de ordem $m \times n$. Resolvendo o producto de Kronecker de matrizes obtidas da construção de Paley e a matriz $2 \times 2$,

$$\boldsymbol{H} \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

podem obter-se matrizes de Hadamard de todas as ordens até 100 com exceção de 92. (Lint, J. H. V.; Wilson & R. M., 2002).

Combinada com pesquisas realizadas em computador, uma matriz de tamanho 92 foi construída, em 1962, por Baumert, Golomb, e por Hall, utilizando uma estrutura original de Williamson, ( Baumert, L.; Golomb, S. W. & Marshall Hall, Jr., 1962).

As matrizes de Hadamard são reconhecidas por possuírem muitas ordens possíveis. A menor ordem para a qual ainda não se sabe se existe uma matriz de Hadamard é a 668. Uma solução para o caso 428 foi obtida por Kharaghani e Tayfeh-Rezaie em Junho de 2004, (Kharaghani, H. & Tayfeh-Rezaie, B., 2004).

Exemplos de matrizes de Hadamard foram construídos por James Joseph Sylvester, (Sylvester, J. J., 1867). Se $\boldsymbol{H}$ for uma matriz de Hadamard de ordem $n$, então a matriz particionada é dada por:

$$\boldsymbol{H} \equiv \begin{bmatrix} H & H \\ H & -H \end{bmatrix}.$$

Esta é uma matriz de Hadamard de ordem $2n$. Esta observação pode ser aplicada de forma repetida e leva ao desenvolvimento da seguinte sequência de matrizes denominada matrizes de Walsh,

$$\boldsymbol{H_1} \equiv [1]$$

$$\boldsymbol{H_2} \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$\boldsymbol{H_{2^k}} \equiv \begin{bmatrix} H_{\boldsymbol{2^k-1}} & H_{\boldsymbol{2^k-1}} \\ H_{\boldsymbol{2^k-1}} & -H_{\boldsymbol{2^k-1}} \end{bmatrix} \equiv \boldsymbol{H_2} \otimes \boldsymbol{H_{2^k-1}},$$

para $2 \leq k \in N$, onde $\otimes$ denota o produto Kronecker (tensor). Desta forma existem as matrizes de Hadamard construídas por (Sylvester, J. J., 1867), de ordem $2^k$ para todos os inteiros não negativos $k$.

## 4.5 – Códigos Cocíclicos de Hadamard

Muitos códigos são construídos a partir de matrizes de Hadamard ou a partir de delineamentos por blocos simétricos relacionados ou conjuntos de diferenças. Estes incluem as três construções de códigos binários de Hadamard da versão $\boldsymbol{H}$ de uma matriz de Hadamard binária. Quando a matriz de Hadamard utilizada para as construções é cocíclica, os códigos resultantes são da categoria I.

Por conseguinte, os códigos de Reed-Muller *simplex* e de primeira ordem (construídos a partir de matrizes de Hadamard do tipo Sylvester) e os códigos de resíduos quadráticos alargados (construídos a partir de matrizes de Hadamard do tipo Paley) são códigos de Hadamard binários cocíclicos.

## 4.6 – Códigos de resíduos quadráticos

Um código de resíduos quadráticos (QR Code - não deve ser confundido com os códigos de resposta rápida) é um tipo de código cíclico. Um código cíclico é como um código binário, que muda apenas um dígito quando se passa de um número para o número imediatamente a seguir, e nesse dígito em apenas uma unidade.

Existe um código de resíduos quadráticos de comprimento $p$ sobre o campo finito $GF(l)$ sempre que $p$ e $l$ são numeros primos, $p$ é ímpar e $l$ é um resíduo quadrático módulo $p$. O gerador polinomial como código cíclico é dado por,

$$f(x) \equiv \prod_{j \in Q} (x - \varsigma^j)$$

onde $Q$ é o conjunto de resíduos quadráticos de $p$ no conjunto {1,2,…, $p$-1} e $\varsigma$ é uma raiz primitiva de ordem $p$ de unidade nalgum campo de extensão finita de $GF(l)$.

A condição de que $l$ é um resíduo quadrático de $p$ garante que os coeficientes de $f$ se insiram em $GF(l)$. A dimensão do código é $(p+1)/2$.

Substituindo $\varsigma$ por outra raiz primitiva de ordem $p$ de unidade $\varsigma^\tau$ ambas resultam no mesmo código ou num código equivalente, de acordo com $\tau$ ser ou não um resíduo quadrático de $p$.

Adicionando um dígito de paridade a um código de resíduos quadráticos obtém-se um código de resíduos quadráticos estendido. Exemplos de códigos de resíduos quadráticos incluem o código Hamming (7,4) de correção de erros sobre $GF(2)$, o código binário de Golay (23,12) sobre $GF(2)$ e o código ternário (11,6) de Golay sobre $GF(3)$.

Os códigos de resíduos quadráticos são obtidos a partir de matrizes de Hadamard enviesadas do tipo Paley.

## 4.7 – Exemplos de matrizes de Hadamard.

Como apresentado na Secção 4.4. um exemplo de uma Matriz 2×2 de Hadamard:

$$H_2 \equiv \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Matriz 4×4 de Hadamard:

$$H_4 \equiv \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right]$$

Matriz 8×8 de Hadamard:

$$H_8 \equiv \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right].$$

## 4.8 – Ligação entre as matrizes de Hadamard e os BIBD

Considere-se uma matriz de Hadamard $H_{4u}$, a qual sem perda de generalidade se considera estar na sua forma usual.
Elimine-se de $H_{4u}$ a primeira linha e a primeira coluna, ambas compostas por 1's e obtém-se a matriz $A$ de ordem $(4u - 1) \times (4u - 1)$.
Define-se, $N \equiv \frac{1}{2}(A + J_{4u-1})$. Isto significa que $N$ é obtida de $A$, substituindo os $-1$'s em $A$ por zero e mantendo os $+1$'s inalterados.

Assim sendo verifica-se que $N$ é a matriz de incidência de um BIBD com parâmetros:

$$v \equiv 4u - 1 \equiv b \, ; r \equiv 2u - 1 \; e \; \lambda - 1.$$

De forma análoga, se M é a matriz de incidência de um BIBD com parâmetros dados anteriormente, então substituindo os zeros da matriz M por $-1$ e acrescentando à matriz resultante uma linha e coluna de 1's, obtém-se a matriz de ordem 4u.
Temos assim o seguinte teorema:

**Teorema**:
A existência de uma matriz de Hadamard de ordem 4u é equivalente à existência de um BIBD com parâmetros dados anteriormente.

**Exemplo 1** - Considere-se uma matriz de Hadamard $\boldsymbol{H}_{16}$ a qual pode ser obtida através do produto tensor $\boldsymbol{H}_4 \otimes \boldsymbol{H}_4$ , onde $\boldsymbol{H}_4$ é dada por:

$$H_4 \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Ao seguirmos o método de construção, descrito acima, obtém-se um BIBD com parâmetros $v \equiv 15 \equiv b$ , $r \equiv 7 \equiv k$ , $\lambda \equiv 3$.

Nos exemplos seguintes mostra-se o produto de Kronecker de $\boldsymbol{H}_4$ por $\boldsymbol{H}_4$, bem como a matriz de incidência para o BIBD (15,15,7,7,3).

Produto de Kronecker de $H_4$ por $H_4$ e matriz de incidência do BIBD:

$$\boldsymbol{H_4 \otimes H_4} =$$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 |
| 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 |
| 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 |
| 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 |
| 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 |
| 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |
| 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 |
| 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 |
| 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 |
| 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 |
| 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 |
| 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 |
| 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 |

Produto de Kronecker de $H_4$ por $H_4$

$$\boldsymbol{N} =$$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | |

Matriz de incidência do BIBD

## 4.9 – Utilização das matrizes de Hadamard na correção de erros

Os códigos de Reed-Muller são uma família de códigos lineares, utilizados na correção de erros. São muito utilizados nas comunicações e foram descobertos por Irving S. Reed e David E. Muller, os quais em 1954 publicaram de forma independente dois artigos acerca destes códigos, (Reed, I. S. & Muller, D. E, 1954).

Muller descobriu os códigos e Reed propôs a maioria da lógica de descodificação. Casos especiais de códigos de Reed-Muller incluem o código de Hadamard, o código de Walsh-Hadamard, e o código Reed-Solomon.

O código de Hadamard é um código utilizado para a deteção e correção de erros na transmissão de mensagens através de canais com muito ruído ou pouco confiáveis. Uma famosa aplicação do código Hadamard foi na sonda espacial Mariner 9 da NASA em 1971, em que o código foi usado para transmitir fotos de Marte para a Terra.

Os códigos de Hadamard generalizados são obtidos a partir de uma matriz de Hadamard $H,\ n \times n$. Em particular, as *codewords* $2n$ do código são as linhas de $H$ e as linhas de $-H$. Para obter um código com o alfabeto $\{0\ ,1\}$, o mapeamento $-1 \rightarrow 1$, $1 \rightarrow 0$, ou, de forma equivalente, $x \rightarrow (1\ -\ x)/2$, é aplicado aos elementos da matriz.

A distância mínima do código é $n/2$. Isso advém da propriedade da definição de matrizes de Hadamard, que afirma que as linhas destas são ortogonais entre si. Isto implica que duas linhas distintas de uma matriz de Hadamard diferem em exatamente $n/2$ posições e, como a negação de uma linha não afeta a ortogonalidade, qualquer linha de $H$ também difere de qualquer linha de $-H$ em $n/2$ posições, excepto quando as linhas correspondem, e nesse caso elas diferem em $n$ posições.

Para obter o código Hadamard acima com $n \equiv 2^{k-1}$, a matriz de Hadamard escolhida $H$ tem que ser do tipo Sylvester, o que dá origem a um comprimento de mensagem $log_2(2n)$. As matrizes terão de ser do tipo Sylvester pois estas permitem o desenvolvimento das palavras binárias que formam o código. Uma matriz Hadamard do tipo Sylvester é uma matriz quadrada de elementos $\pm 1$, cujos vetores, representados pelas linhas distintas da matriz, são ortogonais, ou seja o seu produto interno é zero. Estas são portanto matrizes de Hadamard de ordem igual a $2p$ onde $p$ é um número inteiro positivo, como por exemplo:

$$H_1 = [1]$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

A matriz de Hadamard do tipo Sylvester de ordem $N = 2p$, é gerada através da utilização recursiva da fórmula:

$$H_1 = [1] \quad ; H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ e } HN = H2 \otimes HN/2,$$

onde $\otimes$ denota o produto de Kronecker, que se define da seguinte forma:

Se $A = [a_{ij}]$ é uma matriz $n1$ por $m1$ e $B = [b_{ij}]$ é uma matriz $n2$ por $m2$, então o produto de Kronecker $A \otimes B$ é a matriz:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & . & . & . & a_{1m1}B \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ a_{n11}B & a_{n12}B & . & . & . & a_{n1m1}B \end{bmatrix}.$$

Nas matrizes de Hadamard do tipo Sylvester, $4m \times 4m$, $H_{4m}$, $-H_{4m}$ e, modificando-lhes todos os elementos $-1$ para 0's, segue-se:

$H_{4m} \rightarrow \widehat{H}_{4m} = [-H_{4m} + 2\,J_{4m}] \ \ mod\ 3$ e $-H_{4m} \rightarrow \widehat{H'}_{4m} = [H_{4m} + 2\,J_{4m}] \ \ mod\ 3$,

onde $J_{4m}$ é a matriz $4m \times 4m$, cujos elementos são todos 1's. Isto devolve como resultado palavras binárias de comprimento 4m.

Os códigos binários que são construídos utilizando 8m linhas de $\widehat{H}_{4m}$ e de $\widehat{H}'_{4m}$ são chamados códigos de Hadamard. Um exemplo de um código de Hadamard de ordem 16, utilizando:

$H_8 = H_2 \otimes H_2 \otimes H_2$ , pode ser visto abaixo:

$$C_8 = \left\{ \begin{matrix} 1111\ 1111, 1010\ 1010, 1100\ 1100, 1001\ 1001, 1111\ 0000, 1010\ 0101, 1100\ 0011, 1001\ 0110, \\ 0000\ 0000, 0101\ 0101, 0011\ 0011, 0110\ 0110, 0000\ 1111, 0101\ 10110, 0011\ 1100, 0110\ 1001 \end{matrix} \right\};$$

QR-Codes contêm palavras-código com 8 bits de comprimento e usam o algoritmo de correção de erros Reed-Solomon, com quatro níveis diferentes de correção de erros. Quanto maior o nível de correção de erros selecionado menor será a capacidade de armazenamento disponível no QR-Code.

O algoritmo de Reed-Solomon foi criado por Irving Reed e Gustave Solomon, ambos engenheiros do Lincoln Labs no MIT. Consultar, ( Reed, I. S. & Solomon, G. 1960).
Os códigos de Reed-Solomon são da mesma família de códigos de correção de erros que os códigos de Hadamard.

As linhas de uma matriz geradora $k \times v$, de um código de Reed Solomon (RS) generalizado, $\mathrm{GR_k}(\mathrm{c}, 1)$, onde $\mathrm{c} \equiv (1, \mathrm{c}, \ldots, \mathrm{c}^{\mathrm{v}-1})$ para algum $\mathrm{c} \in \mathrm{GF}(\mathrm{q})$, de ordem v, são linhas de uma matriz cocíclica.

Para $v \equiv p$, um número primo ímpar, os códigos Reed-Solomon resultantes são códigos cocíclicos de Hadamard. Assim sendo, os códigos de Reed-Solomon também estão intimamente relacionados com as matrizes de Hadamard.

# Capítulo 5

# Códigos QR, Risco e novas tecnologias

## 5.1 – Risco associado a Códigos QR

Risco é o potencial de perder algo de valor, avaliado contra o potencial para ganhar algo de valor. O risco é também uma probabilidade ou ameaça de dano, prejuízo, responsabilidade, perda ou qualquer outra ocorrência negativa que é provocada por vulnerabilidades externas ou internas, as quais podem ser evitadas através de uma ação preventiva. Existem vários tipos de risco, ou seja, diferentes classes ou várias formas de risco, tais como: risco presente num projeto, que são os fatores que podem causar que um projeto fracasse; o risco do negócio, que está associado com o nível de exposição que uma empresa irá enfrentar se um projeto falhar; o risco nos sistemas de produção, que considera os custos de funcionamento de um projeto; o risco económico, que se pode manifestar em menores rendimentos ou despesas mais elevadas do que o esperado; a saúde; a segurança e o risco ambiental.

Mesmo que estas sejam áreas separadas, encontram-se muitas vezes relacionadas porque um único evento pode ter impacto em todas essas três áreas. Outros tipos de risco são o risco de segurança que diz respeito à proteção dos ativos de danos causados por atos deliberados, risco inerente a tecnologia da informação e risco de segurança da informação, entre muitos outros. O tipo de risco que mais concerne aos Códigos QR é o risco de segurança da informação na sua vertente de risco de perda de informação. Aqui, o risco de perda de informação refere-se à problemática da perda de dados importantes, contidos no Código QR.

A avaliação de risco é o processo de identificação de potenciais riscos e de análise do que pode acontecer se ocorrer um perigo. Um perigo é uma ameaça reconhecida. Portanto a avaliação de risco é a determinação do valor quantitativo ou qualitativo do risco relacionado com uma situação concreta e uma ameaça reconhecida. Existem vários métodos para a realização de uma avaliação de risco, no entanto, há um que se acredita ser o mais simples para a maioria das organizações. Este método consiste em cinco

etapas: identificar os perigos, decidir quem poderá ser prejudicado e como, avaliar os riscos e decidir sobre as precauções a tomar, anotar os resultados e implementá-los e a etapa final consiste em rever a avaliação e atualizá-la, se necessário. As avaliações de risco quantitativas incluem um cálculo da expetativa de perda única (SLE - *single loss expectancy*), de um recurso.

A expectativa de perda única (SLE) é definida como o valor monetário esperado a partir da ocorrência de um risco de um ativo e está matematicamente definida como: $SLE \equiv Valor\ do\ ativo \times Fator\ de\ Exposição$. O fator de exposição é representado no impacto do risco sobre o ativo considerado, ou como uma percentagem de perda do ativo. Ilustrando com um exemplo, se o valor do ativo é reduzido em um terço, o valor do fator de exposição é 0,33. Se o ativo é completamente perdido, o fator de exposição é de 1,0 (ou seja, 100%). O resultado da fórmula anterior é um valor monetário, representado na mesma unidade que a expetativa de perda única, ou seja é expressa em euros, dólares, ienes, etc.

Garantia da informação é a prática de assegurar os riscos de informação e de gestão relacionadas com o uso, processamento, armazenamento e transmissão de informações ou de dados e os sistemas e processos utilizados para esses fins. Para os Códigos QR existe um risco significativo de dano e, portanto, o risco de perda das informações neste contidas. Como exemplo, uma avaliação de risco pode ser determinada para um Código QR. Este Código QR em particular é assumido como fazendo parte de uma campanha publicitária e este supõe-se exposto aos elementos climatéricos, portanto, a possibilidade de danos a este código é aumentada. Aqui, o fator de exposição é assumido como sendo 0,30, ou seja, o código suporta um dano de 30%. O ativo é assumido como sendo realmente valioso para a empresa que realiza a campanha de publicidade, portanto, a expectativa de perda única ou SLE é, considerando os fatores anteriores, também elevada. Por isso, é muito importante tentar manter as informações contidas no Código QR o mais recuperáveis possível, mesmo sob estas condições de risco. Para evitar a perda de informações neste Código QR um maior nível de correção de erros deve ser selecionado quando o código é criado. Existem quatro níveis de correção de erros que podem ser usados: Nível L → a informação é recuperável até 7% de danos, Nível M → até 15% de danos, Nível Q → até 25% de danos e Nível H → até

30% de danos. Estes valores estão descritos na norma internacional ISO/IEC 18004: 2006 (E) secção 8.5.1, Tabela 12.

Em condições adversas, onde o Código QR está exposto aos elementos, tais como a chuva, vento, sol, poeira, etc. o nível H deve ser usado. Por isso, mesmo que tenha existido 30% de danos provocados num Código QR, as informações nele contidas ainda seriam totalmente legíveis. Como tal, quando se constroem Códigos QR para, por exemplo, cartões-de-visita, a probabilidade de este ficar sujo são consideravelmente baixas e é desejável ter um Código QR tão pequeno quanto possível. Aqui, um limiar padrão de erro de 7% é suficiente e considera-se adequado.

No entanto, se os Códigos QR são produzidos para utilização ao ar livre, para por exemplo colocar em carros e camiões ou em qualquer lugar onde os dados podem ser obscurecidos por poluição, então um nível de correção de erros com uma configuração mais alta é aconselhável.

Infelizmente, quanto maior for o nível de correção de erros que é usado menos informação pode ser escrita no Código QR. Portanto, há um compromisso entre a mitigação de risco e o fornecimento de informações.

## 5.2 – Exemplos de Códigos QR

Os Códigos QR podem representar texto, um endereço para um site (*URL*), um número de telefone, uma localização georreferenciada, um *e-mail*, um contacto ou um *SMS*. Inicialmente estes códigos foram utilizados para catalogar peças na produção de veículos.

Desde que foi inventado o Código QR tem sido utilizado para as mais variadas funções, no entanto, nos últimos anos, a sua utilização tem estado muito associada a ações de *marketing* e comunicação, fazendo uma ponte de ligação entre a comunicação *online* e a comunicação *offline*.

Em Portugal foi desenvolvido, em 2012, um projeto inovador que resultou de um trabalho de uma agência de comunicação, a *MSTF Partners*, para o Turismo de Portugal e para a Associação de Valorização do Chiado que consistia na utilização de um Código QR em calçada portuguesa, que se pode observar na Figura 1, com o objetivo de divulgar Lisboa enquanto destino turístico. A ideia foi fazer um Código QR, uma das

tecnologias com maior potencial do século XXI, com pedras de calçada portuguesa, uma das mais antigas tradições portuguesas.

**Figura 1** – Exemplo de código QR, construído em calçada Portuguesa
Fonte: http://boasnoticias.pt/mobile/noticias.php?id=12470

"*Acabou de ler o primeiro código QR do mundo feito em calçada portuguesa*", disponível em português e em inglês, é a mensagem inicial que aparece ao entrar nesta experiência. Num segundo nível de informação foram acrescentados conteúdos de informação turística e comercial sobre a oferta cultural, gastronómica, hoteleira e de comércio no Chiado.

O sucesso do Código QR em calçada portuguesa foi de tal modo grande que atravessou o Atlântico e foi implementado, em 2013, no calçadão das praias do Rio de Janeiro, o que permite aos turistas ampliar o conhecimento sobre a cidade maravilhosa através de um novo recurso tecnológico. Ao aproximar o telemóvel, o utilizador poderá receber informações como a origem do nome da região ou a agenda de atividades turísticas, como os locais ideais para ver o pôr-do-sol no local ou visitar um museu próximo, ou ainda informações culturais, gastronómicas e comerciais.

Outro exemplo de Código QR pode ser observado nas embalagens de pastéis de Belém. Estes códigos continham uma hiperligação para uma página *web* que falava acerca de outro dos nossos grandes marcos culturais, o Fado, Figura 2:


**Figura 2** – Código QR presente numa embalagem de pastéis de Belém

**Fonte**: http://lisboanoguiness.blogs.sapo.pt/256887.html

Um outro exemplo é o Código QR que se apresenta na Figura 3. Este contém a hiperligação para a conferência internacional da Amazónia em estatística experimental e análise de risco.

**Figura 3** – Código QR que contém a hiperligação para a conferência Manaus 2014.

### 5.3 – Como gerar Códigos QR *online*

Os Códigos QR, apesar de parecerem complexos, podem ser criados por qualquer pessoa interessada em fazê-lo.

Existem vários *sites* na Internet onde é possível produzir Códigos QR, desde os mais simples até aos mais ornamentados. Como primeiro passo para a elaboração do Código QR sugere-se a elaboração da mensagem que se pretende codificar. Esta pode conter, como dito anteriormente, texto simples, uma hiperligação, um número de telefone ou informações completas de contacto pessoal, um *sms* semelhante aos recebidos nos telemóveis, um cartão-de-visita digital, um *e-mail*, entre outros.

A norma ISO/IEC 18004:2006 permite que se codifiquem até 4296 carateres alfanuméricos (caracteres de 0 a 9, letras de A a Z, e outros caracteres como um espaço ou $, %, *, +, -, ., / e :) ou 7089 carateres numéricos (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), num Código QR.

Uma breve pesquisa efetuada no motor de procura Google, introduzindo os termos QR Code generator, devolve várias páginas dedicadas à geração de Códigos QR. A seguir apresenta-se uma lista resumida de alguns dos possíveis *sites* para elaborar códigos QR bem como uma breve descrição das diferentes funcionalidades presentes nessas páginas web.

- www.the-qrcode-generator.com, nesta página é possível elaborar um código QR simples, sem cores ou quaisquer outros ornamentos, para tal basta seguir dois simples passos: seleciona-se da lista à esquerda o tipo de Código QR pretendido, este pode ser texto simples, uma hiperligação, etc. e de seguida introduz-se na caixa de texto, ao centro, a mensagem que se deseja codificar no Código QR, automaticamente o *site* gera, à direita, o código QR correspondente. Este pode ser gravado para o computador através do botão *Save* (cor de laranja) presente por cima do Código QR gerado. Apresenta-se a seguir um exemplo de um Código QR concebido neste *site*, Figura 4:

**Exemplo:**

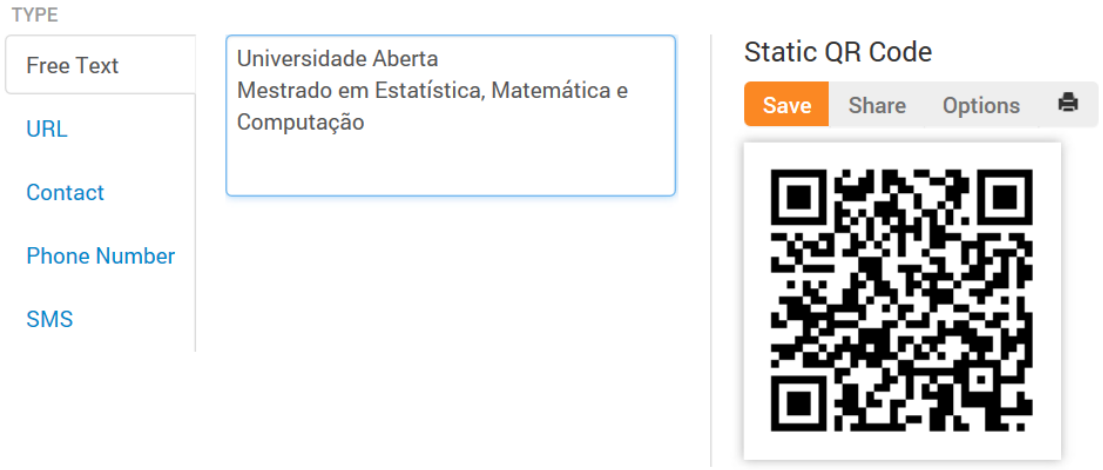



**Figura 4** – Código QR gerado na página www.the-qrcode-generator.com

- www.qrstuff.com, esta página apresenta uma vertente mais comercial do que a anterior. Nesta página é possível elaborar um código QR mais complexo que o anterior, recorrendo à utilização de cores. É ainda possível, para além de se guardar, de forma gratuita, o Código QR no computador, incluir o mesmo em objetos tais como um boné, uma caneca ou um pin, mediante o pagamento do serviço correspondente. A rotina a seguir para se elaborar o código QR é muito semelhante à descrita para o *site* anterior, contudo possuí um passo adicional, a seleção da cor do Código QR. Começa-se por se selecionar o tipo de Código QR pretendido na lista presente à esquerda, de seguida introduz-se na caixa de texto, ao centro, a mensagem que se deseja codificar, depois seleciona-se a cor que se deseja que o código apresente e automaticamente o *site* gera, à direita, o código QR correspondente. Como último passo, referenciado na imagem seguinte como passo 4, pode fazer-se o *download* do código para o computador ou utilizar o serviço que o permite colocar num objeto. Apresenta-se a seguir um exemplo de um Código QR concebido nesta página *web*, Figura 5:

**Exemplo:**

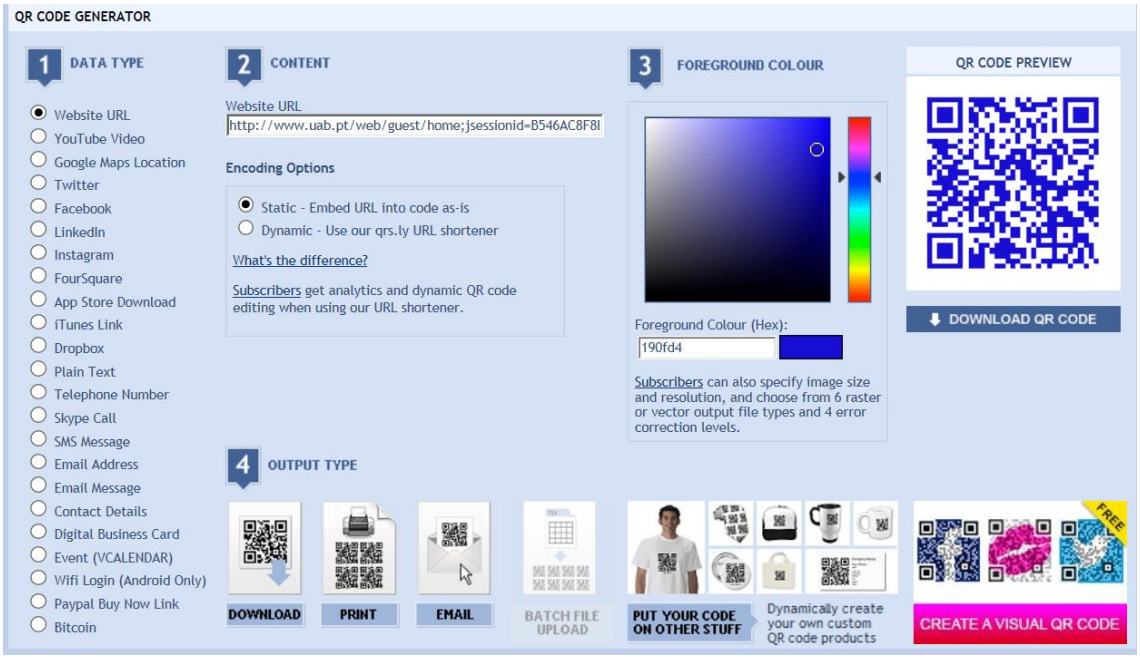



**Figura 5** – Código QR gerado na página www.qrstuff.com

- www.aptika.com/qrcode, nesta página é possível criar um código QR semelhante ao da página anterior, ou seja com recurso à utilização de cor. Contudo nesta página é adicionada a funcionalidade que permite definir o tamanho, em *pixels*, que se deseja para o código gerado. O procedimento a seguir para obter o código é semelhante aos anteriores, escolhe-se da lista à esquerda o tipo de código e de seguida introduz-se a mensagem a codificar, depois escolhe-se o tamanho que se deseja para o código e a cor que o mesmo deve apresentar. Finalmente, deve-se pressionar o botão *Create QR-Code* e o *site* apresentará, à direita, o código QR gerado. Um exemplo de um Código QR concebido nesta página web é mostrado a seguir, Figura 6:

**Exemplo:**

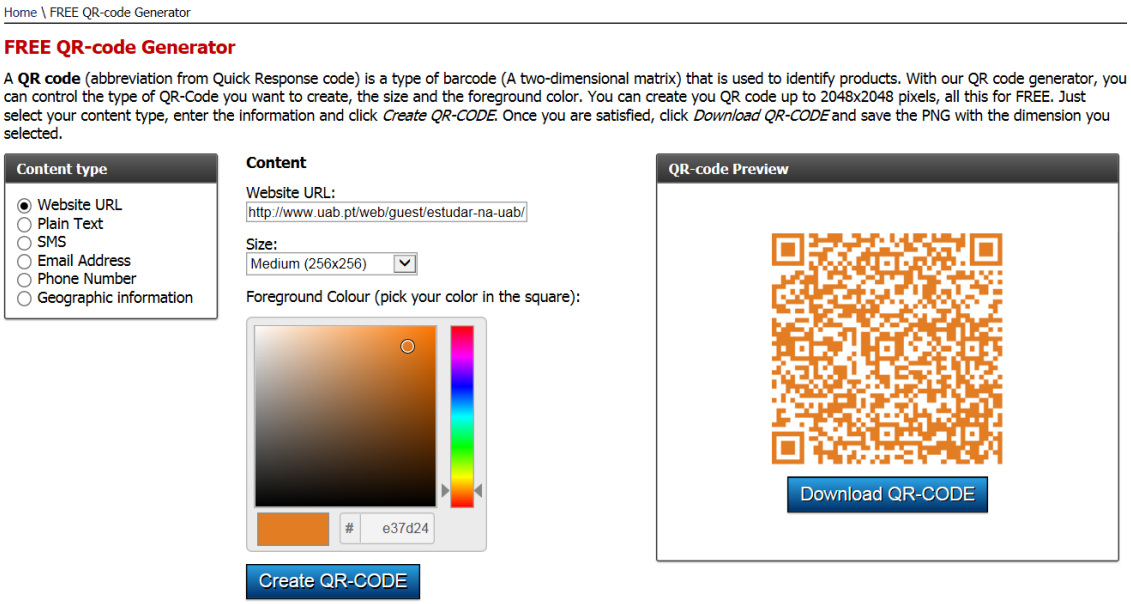



**Figura 6** – Código QR gerado na página www.aptika.com/qrcode

- http://goqr.me, esta página permite apenas a elaboração de Códigos QR simples, a preto e branco, contudo possui uma vertente comercial que permite a inclusão de um logotipo sobre o Código QR produzido.

  O procedimento para se obter o código é semelhante aos anteriores, escolhe-se dos ícones presentes à esquerda da página o tipo de código pretendido e de seguida introduz-se a mensagem a codificar e de forma automática a página apresenta o código gerado, à direita. Pode guardar-se este código utilizando o botão *Download*.

  Um exemplo de um Código QR concebido nesta página web é mostrado a seguir, Figura 7:

**Exemplo:**

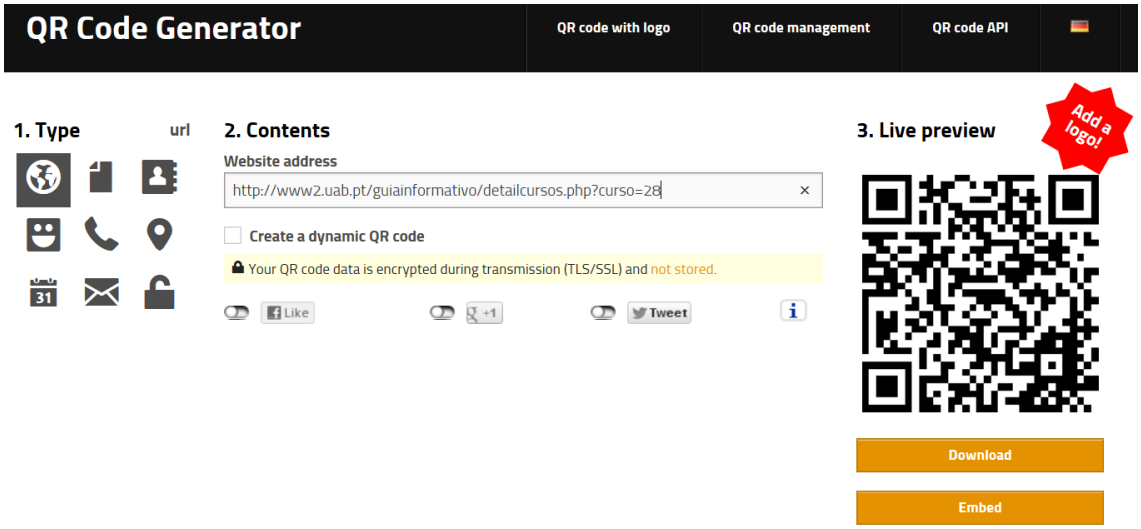



**Figura 7** – Código QR gerado na página http://goqr.me

- www.unitag.io/qrcode, à semelhança das páginas anteriores esta página permite criar Códigos QR com diversos tipos diferentes de conteúdo, contudo este é um dos *sites* que apresenta maior capacidade de customização do Código QR gerado. É possível adicionar ao código gerado cores diversas, logotipos, modelos pré-concebidos, efeitos de sombra, entre várias outras opções.

  Para gerar um Código QR devem seguir-se os passos descritos na página. No passo 1 seleciona-se o tipo do código pretendido e introduz-se na caixa de texto a mensagem a codificar e carrega-se no botão *Confirm*. No passo 2 procede-se à customização do código, utilizando as várias opções presentes.

  No exemplo seguinte apresenta-se um Código QR concebido nesta página, note-se a adição de cor e de um logotipo ao código gerado, Figura 8:

**Exemplo:**

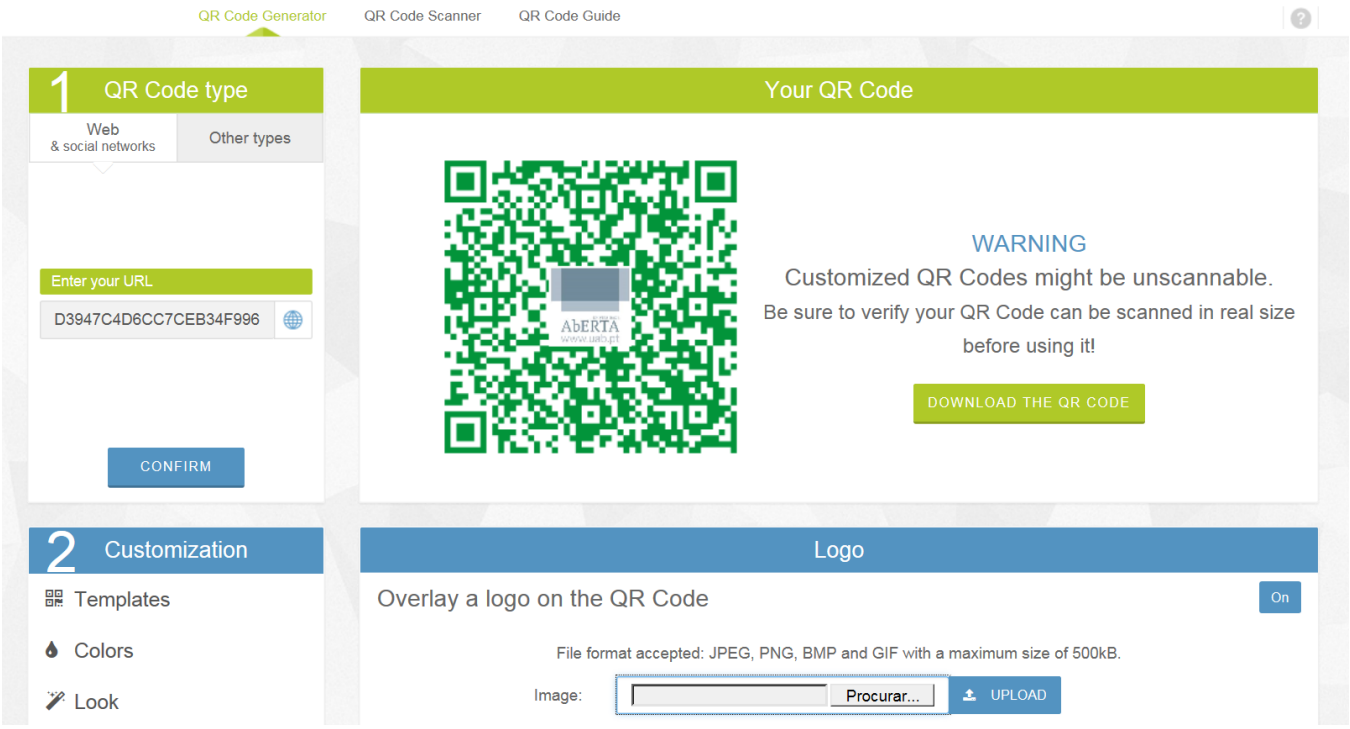



**Figura 8** – Código QR gerado na página [www.unitag.io/qrcode](www.unitag.io/qrcode)

A capa deste trabalho apresenta a imagem de um cubo, elaborado com o auxílio do *software* Photoshop produzido pela empresa Adobe. As 3 faces visíveis estão preenchidas com três Códigos QR, os quais foram gerados na página [www.the-qrcode-generator.com](www.the-qrcode-generator.com) e posteriormente coloridos e dimensionados no Photoshop. Estes Códigos QR contêm, cada um, uma hiperligação para a página institucional da orientadora e co-orientadora e para uma página pessoal da autora desta dissertação. Cada um destes códigos pode ser lido com o auxílio de um telemóvel ou *ipad.*

## 5.4 – Exemplo de correção de erros nos Códigos QR

O exemplo que se segue mostra um Código QR, o qual apesar de danificado ainda é totalmente descodificável, ou seja ainda é perfeitamente legível, graças à utilização dos códigos de correção de erros. Estes códigos, como já foi mencionado anteriormente, fazem parte da família de códigos baseados nas matrizes de Hadamard, as quais por sua vez estão relacionadas com os BIBD.

**Figura 9** – Código QR danificado, ainda é legível devido aos códigos de correção de erros nele presentes.
**Fonte:** WikiPedia. Disponível em: http://commons.wikimedia.org/wiki/File:QR_Code_Damaged.jpg. Acesso em 29/06/2014.

## 5.5 – Biometria associada a Códigos QR

Nas tecnologias da informação, a biometria refere-se a tecnologias para identificar as características do corpo humano, tais como as impressões digitais e as íris dos olhos. No entanto, há uma enorme quantidade de dados de pesquisa que demonstram que os dados biométricos referentes a características físicas de um indivíduo, podem ser falsificados.

Há vários exemplos na Internet sobre como fazer falsas impressões digitais ou como forjar imagens da íris. Grandes empresas como o Facebook estão a fazer esforços para desenvolver tanto *tokens* de *hardware* como de autenticação baseada em *software*, para a sua rede social.

A geração de códigos por *software*, como por exemplo os códigos de resposta rápida (Códigos QR), parece oferecer uma solução preferível, em vez do simples reconhecimento biométrico, isto é conseguido graças às suas propriedades matemáticas as quais acrescentam uma camada de segurança acrescida.

Um engenheiro do Facebook, Gregg Stefancik, declarou numa entrevista que gostaria que a sua empresa se afastasse da utilização de *passwords*, mas contudo opõe-se à utilização da biometria a qual considera insegura. No entanto a segurança biométrica pode ser alavancada com uma solução de autenticação de dois fatores, que se obtém garantindo que as senhas alfanuméricas ou códigos gerados entrem nas etapas de autenticação. Uma combinação de reconhecimento de voz baseado, por exemplo, numa frase, juntamente com um Código QR já é considerada uma solução de autenticação extremamente forte. A Lumidigm, fabricante de máquinas *ATM*, já está a utilizar esse princípio nas suas máquinas. As suas máquinas *ATM* utilizam uma combinação de biometria e de Códigos QR para que se efetuem operações seguras de levantamento de dinheiro.

Na Figura 10, pode ver-se um exemplo de uma destas máquinas a ser utilizada. É necessária a colocação do dedo para ler a impressão digital e também é necessária a utilização de um Código QR para confirmar a autenticação do utilizador:

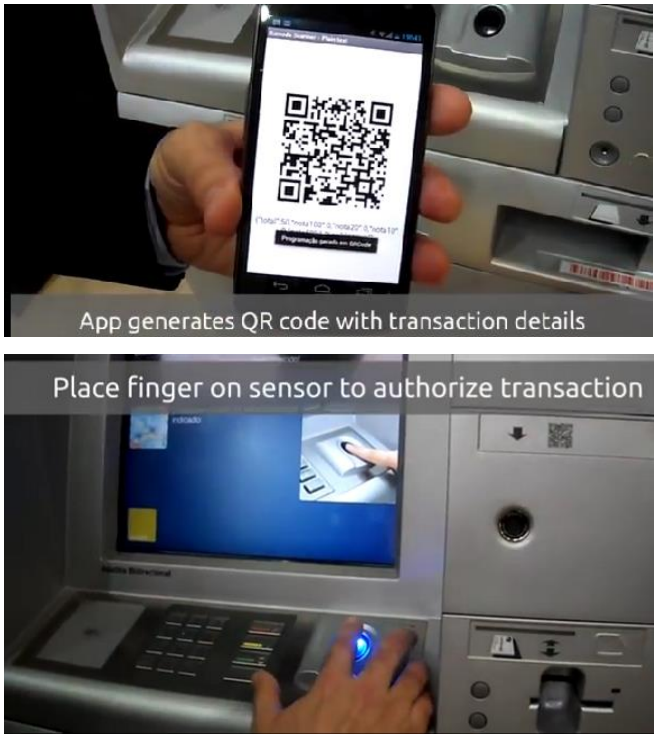



**Figura 10** – Um utilizador que usa um Código QR, gerado por uma aplicação instalada no seu telemóvel, e a sua impressão digital para poder utilizar a máquina *ATM*.

**Fonte:** Estas duas imagens foram obtidas de dois fotogramas do vídeo disponível em: http://www.lumidigm.com/video-withdrawing-cash-from-an-atm-with-a-qr-code-and-a-finger/ .

Acesso em 23/05/2014: *Withdrawing Cash from an ATM with a QR Code and a Finger*

## 5.6 – Criptomoeda

A criptomoeda é um tipo de moeda digital que utiliza criptografia para implementar as necessárias medidas de segurança e de anti-falsificação. Chaves públicas e privadas são muitas vezes utilizadas para garantir a transferência, de forma segura, de criptomoeda entre indivíduos. Uma sequência de números, a qual contém propriedades matemáticas que tornam muito difícil defraudar o sistema, é enviada, via Internet, a partir da pessoa que quer comprar alguma coisa, para a pessoa que está a vender esse bem.

A transação é efetuada através de um pacote de *software* chamado cliente de criptomoeda. É este *software* que gera a sequência de números. Uma das criptomoedas mais conhecidas é a *Bitcoin.* As *Bitcoin* podem ser trocadas por moedas reais, tais como o euro ou o dólar. No momento, em que escrevo uma *bitcoin* vale 100 dólares.

Um dos *sites* de câmbio mais conhecidos é o mtgox.com. No entanto, e ao contrário de uma moeda convencional, não há necessidade de transacionar uma *Bitcoin* inteira, porque esta moeda tem 8 dígitos decimais e pode ser dividida em 0,00000001 unidades. Este número é conhecido por 1 Satoshi.
Um exemplo de criptomoeda com a sua respetiva chave privada pode ser observado na Figura 11:


**Figura 11** – Exemplo de Bitcoin com a sua respectiva chave privada
Fonte: http://coinboxy.com/

As criptomoedas têm um número de propriedades interessantes, por exemplo, utilizando criptomoeda uma pessoa pode permanecer anónima porque a sequência de números, que é trocada, funciona como um pseudónimo para a pessoa que emite o pagamento. Outra propriedade é o facto de estas moedas serem abertas ao público em geral, o que significa que qualquer pessoa pode usá-las. Estas moedas são também descentralizadas, ou seja, este tipo de moedas não têm que ter intermediários, não há nenhum banco envolvido na transação. Devido ao facto destas moedas não estarem vinculadas a um determinado país, o seu valor não é controlado por um banco central, e assim o seu valor é determinado pela oferta e procura, o que significa que estas se comportam como se fossem metais preciosos, como ouro ou a prata.

As criptomoedas foram criadas com base em certos princípios de criptografia. A *Bitcoin* foi a primeira criptomoeda a ser criada, em 2009, depois dessa já numerosas outras

criptomoedas surgiram. *Darkcoin*, *Vertcoin*, *Auroracoin* e *MazaCoin* são alguns dos exemplos de criptomoedas que foram criadas durante o ano de 2014.

Existem também alguns fabricantes que produzem máquinas *ATM* exclusivamente dedicadas às criptomoedas, como é o caso do *ATM* de *Bitcoin* que se pode observar na Figura 12:

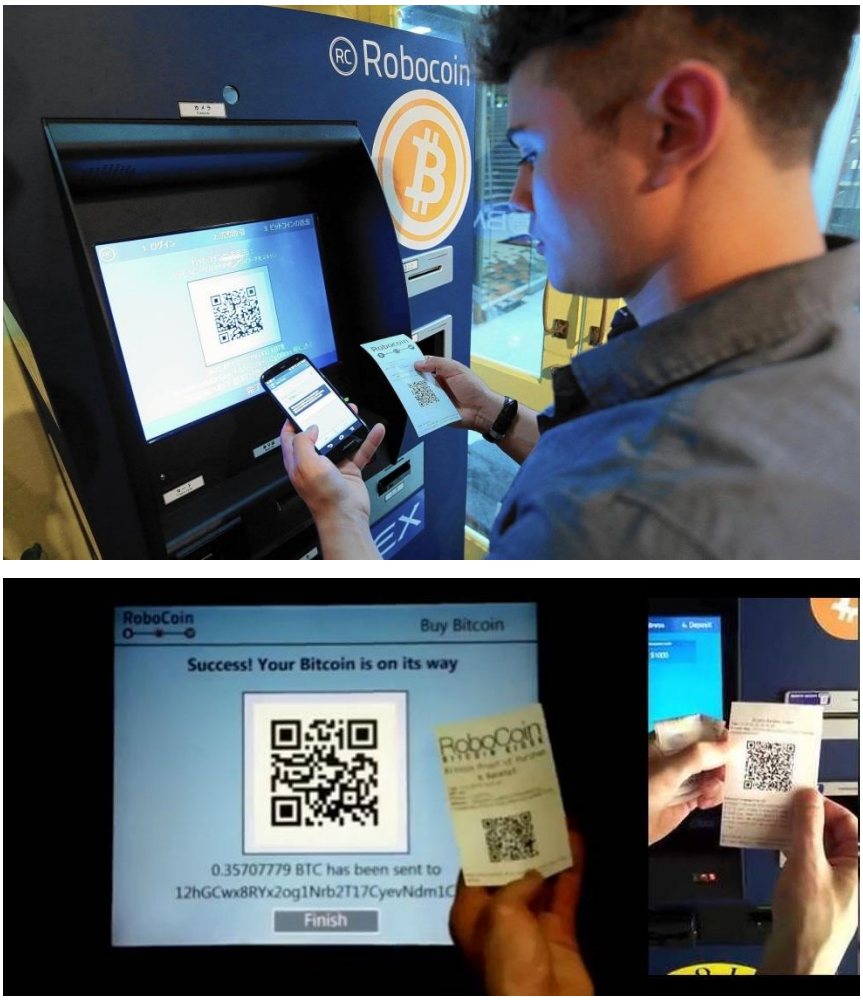



**Figura 12** – Exemplo de um *ATM* de criptomoeda *Bitcoin*
**Fonte:** http://www.tweaktown.com/news/38937/los-angeles-receives-first-bitcoin-atm-machines-courtesy-of-robocoin/

Os Códigos QR também são utilizados para enviar e receber pagamentos com *Bitcoin* em lojas que aceitem criptomoedas como forma de pagamento. Para tal apenas é necessário exibir o Código QR presente na aplicação de carteira *Bitcoin* no telemóvel e

deixar o vendedor ler o respetivo Código QR, ou aproximar dois telemóveis um do outro, efetuando a transação através da tecnologia de rádio NFC.

O pagamento com *Bitcoin* por telemóvel permite efetuar a transação de forma simples e rápida, num processo que envolve dois passos, lê-se o Código QR e confirma-se o pagamento. Assim não existe necessidade de qualquer subscrição de cartões, ou de passar o cartão, digitar um PIN, ou assinar qualquer coisa. As transações *Bitcoin* são protegidas por criptografia de nível militar. Desde que sejam tomados os passos necessários para proteger a respetiva carteira Bitcoin usualmente denominada por *wallet*, a *Bitcoin* assegura controlo total e um forte nível de proteção contra vários tipos de fraude.

O lado negativo é que os Códigos QR podem ser danificados. A maioria das *wallets* em papel inclui a chave privada fisicamente anotada, e esta também pode ser danificada. Deve portanto haver várias cópias. No caso de furto em que os dados da *wallet* não foram devidamente criptografados com BIP38 então as *Bitcoins* armazenadas na *wallet* podem simplesmente desaparecer. Para além disso, devido ao facto de as transações de criptomoeda serem anónimas e não rastreáveis estas criaram um nicho para transações ilegais, como por exemplo o tráfico de drogas e de armas. Como a moeda possui um repositório central, os agentes da lei e processadores de pagamento não têm jurisdição sobre as contas *Bitcoin.* Para quem apoia as criptomoedas, este anonimato é um ponto forte desta tecnologia, apesar do potencial para o abuso ilegal, uma vez que permite uma mudança de poder das instituições para os indivíduos.

As *Bitcoins* são criadas por um *software* especial denominado *software* de mineração, que cria *Bitcoins*, resolvendo equações matemáticas complexas. Os problemas que são resolvidos são de natureza criptográfica. Um número ou frase é transformado num outro número ou noutra frase respetivamente. Um problema de cifra simples é por exemplo a multiplicação de determinados números por 4. Assim, 1 ficaria 4, 2 ficaria 8, 3 ficaria 12, etc. O problema é que se torna fácil descobrir o número original por apenas dividir por 4 e, por conseguinte, isto não seria muito seguro. Para contornar este problema e tornar as criptomoedas seguras, são utilizados algoritmos matemáticos complexos. Estes são chamados funções de *hash* criptográficas.

Uma função *hash* criptográfica é uma função cujos resultados são considerados praticamente impossíveis de reverter, isto é, torna-se impossível recriar os dados de entrada a partir do seu valor de *hash* por si só. Uma função *hash* realiza um mapeamento de um grupo de caracteres, chamado chave, e mapeia-o para um valor de um determinado comprimento, chamado um valor de *hash* ou apenas *hash*. A *Bitcoin* utiliza duas funções *hash*, são elas a SHA-256 e a RIPEMD-160. Para além destas a *Bitcoin* utiliza também uma curva elíptica DSA na curva secp256k1 para produzir assinaturas. A curva secp256k1 específica provém de um padrão com o nome SEC2, publicado por um grupo chamado SECG. Pegando no nome secp256k1 e dividindo-o nos seus componentes, sec vem do padrão, *p* significa que as coordenadas da curva são um campo de números primos (ou seja é um *Galois Field*, GF(p) em que *p* é número primo), 256 significa que o número primo tem 256 bits de comprimento, *k* significa que é uma variante de uma curva *Koblitz* e 1 significa que é a primeira, e única, curva desse tipo na norma. As curvas *Koblitz* são um tipo especial de curvas elípticas que têm uma estrutura interna que pode ser utilizada para acelerar cálculos. A função de *hash* SHA-256 é uma função que é calculada com palavras de 32 bits. RIPEMD-160 é uma versão melhorada, com 160-bits, do original RIPEMD (RACE Integrity Primitives Evaluation Message Digest), onde RACE significa (*Research*) - Pesquisa e Desenvolvimento em Tecnologias Avançadas de Comunicações na Europa. (Preneel, B.; Dobbertin, H. & Bosselaers, A., 1997). Esta função foi gerada na comunidade académica em regime aberto, ou seja todos os interessados puderam dar o seu contributo.

Presentemente toda a documentação referente a esta função encontra-se disponível na página: http://homes.esat.kuleuven.be/~bosselae/ripemd160.html. Nesta página encontra-se também disponível o contacto dos autores Antoon Bosselaers e Bart Preneel, para qualquer esclarecimento adicional.

# Capítulo 6

# Exemplos práticos no R (Project for Statistical Computing)

## 6.1 – Introdução

O *software* R é um conjunto integrado de ferramentas computacionais que permitem a manipulação e análise de dados estatísticos, o cálculo numérico e a produção de gráficos. Para além disto o R é também uma linguagem de programação bem desenvolvida e simples, similar à linguagem S desenvolvida pelos laboratórios Bell por John Chambers e seus colegas. O R pode ser considerado uma implementação diferente da linguagem S.

O R é uma aplicação de distribuição gratuita e de código fonte aberto ao público, existindo versões para execução nos principais sistemas operativos (Windows, Linux e Macintosh). Permite a adição de funcionalidades através do carregamento de pacotes de *software.* Cada um destes pacotes adiciona ao R várias funções com fins específicos.

O projeto R para computação estatística pode ser encontrado na internet na página: www.r-project.org. Na página anterior pode ser encontrado um link para uma outra página, a página do CRAN - The Comprehensive R Archive Network. Esta agrega toda a informação acerca dos vários 'pacotes' existentes relacionados com o desenho experimental com o auxílio do R. Esta página pode também ser acedida diretamente no url: http://cran.r-project.org/web/views/ExperimentalDesign.html. Nesta página são apresentados primeiro os pacotes de utilização genérica e prossegue para os de tarefas específicas como por exemplo os que são utilizados no desenho de experiências para a agricultura, indústria e ensaios clínicos entre outros. Para gerar planos de blocos incompletos equilibrados, com o auxílio computacional do programa estatístico, R pode utilizar-se o pacote adicional, *crossdes*. Este pacote inclui várias funções que auxiliam na construção de planos equilibrados. Cada BIBD produzido, com o auxílio deste pacote, possui cinco parâmetros, a saber: o número de tratamentos, o número de repetições de cada tratamento, o número de blocos, o número de observações e um parâmetro, lambda, que guarda o número de blocos onde ocorre cada par de tratamentos, no plano. Para instalar o pacote utiliza-se o comando: *install.packages* ("*crossdes*") e para utilizar as funções neste contidas, utiliza-se o comando:

*library("crossdes")*. Utiliza-se a função *find.BIB* para gerar um plano de blocos com um número específico de tratamentos, blocos (que correspondem às linhas do plano gerado) e elementos por bloco (que correspondem às colunas do plano gerado).

## 6.2 – Exemplos de geração e confirmação de BIBD com R

É possível utilizar uma outra função, para testar se o plano gerado satisfaz as condições para ser um BIBD. Exemplificando, para criar um plano com cinco tratamentos em quatro blocos de três elementos utiliza-se a função da seguinte forma:

> find.BIB(5, 4, 3)

Resposta do R, na Figura 13:

```
     [,1] [,2] [,3]
[1,]    2    3    5
[2,]    1    2    4
[3,]    3    4    5
[4,]    1    3    5
```

**Figura 13** – Resposta do R, possível BIB 5,4,3

Este desenho experimental não é um BIBD pois os tratamentos não se encontram todos repetidos o mesmo número de vezes.

Esta observação pode ser confirmada através da utilização da função *isGYD*, da seguinte forma: *isGYD(find.BIB(5, 4, 3))*. O resultado da execução desta função no 'R' é dado pelo seguinte *output*, Figura 14:

```
> isGYD(find.BIB(5, 4, 3))
[1] The design is neither balanced w.r.t. rows nor w.r.t. columns.
```

**Figura 14** – Resposta do R, o resultado da função *isGYD* mostra que o BIB não existe

Considere-se agora um outro exemplo, desta vez com sete tratamentos e sete blocos de três elementos, Figura 15:

```
> outro.plano = find.BIB(7, 7, 3)
> outro.plano
     [,1] [,2] [,3]
[1,]    1    2    6
[2,]    3    5    6
[3,]    4    6    7
[4,]    2    3    7
[5,]    1    3    4
[6,]    2    4    5
[7,]    1    5    7
```

**Figura 15** – Resposta do R, possível BIB 7,7,3

Confirma-se através da utilização da função *isGYD*, que este desenho experimental é um BIBD, Figura 16:

```
> isGYD(outro.plano)

[1] The design is a balanced incomplete block design w.r.t. rows.
```

**Figura 16** – Resposta do R, o resultado da função *isGYD* mostra que este BIB existe.

Um outro pacote útil para gerar esboços da distribuição de planos de blocos equilibrados, é o *dae*. Tal como o anterior este apresenta diversas funções orientadas no auxílio em desenho experimental. O exemplo abaixo, Figura 17, ilustra a utilização de uma das funções presentes no *dae*, a *fac.layout* para gerar uma experiência de blocos equilibrados que consiste de fatores aleatórios:

```
> BIBD.unit<-list(Blocks=4, Plots=3)
> BIBD.nest<-list(Plots="Blocks")
> Treats<-factor(c(1,2,3, 1,2,4, 1,3,4, 2,3,4), labels=c("A","B","C","D"))
> BIBD.lay<-fac.layout(unrandomized=BIBD.unit, nested.factors=BIBD.nest, randomized=Treats, seed=987)
> BIBD.lay
   Units Permutation Blocks Plots Treats
1      1           2      1     1      C
2      2           3      1     2      A
3      3           1      1     3      B
4      4          10      2     1      B
5      5          12      2     2      C
6      6          11      2     3      D
7      7           9      3     1      C
8      8           7      3     2      D
9      9           8      3     3      A
10    10           4      4     1      A
11    11           5      4     2      D
12    12           6      4     3      B
>
```

**Figura 17** – Resposta do R, BIBD com fatores aleatórios produzido pela função fac.layout .

# Capítulo 7

# Alguns trabalhos de investigação Recentes

Os BIBD têm sido fundamentais para o desenvolvimento da ciência nas mais variadas áreas de investigação. Apresentam-se a seguir alguns trabalhos recentes desenvolvidos nalgumas destas áreas.

## Biometria

Francisco, C. & Oliveira, T. A., apresentam em 2014 o artigo, *The importance of QR Codes versus Biometrics authentication: Reviewing links to Block Designs*, no 44th International Biometrical Colloquium and 4th Polish-Portuguese Workshop on Biometry 2014, Kraków, Poland, onde discutem a problemática de os códigos de resposta rápida (Códigos QR) serem uma solução preferível ao invés do reconhecimento biométrico, uma vez que pelas suas propriedades matemáticas oferecem uma maior segurança.

## Criptografia

No trabalho apresentado por Ogata, E. et al. em 2004, *New combinatorial designs and their applications to authentication codes and secret sharing schemes,* são exibidos três novos tipos de delineamentos, com base em análise combinatória. Estes são: *External Difference Families* (EDF), *External* BIBD (EBIBD) e *Splitting* BIBD (SBIBD). São apresentadas aplicações destes novos delineamentos aos códigos de autenticação e esquemas de partilha de segredos com segurança robusta, anti-hackers. É ainda exposta a importância da utilização do *software R* no âmbito da criptografia.

A Análise Combinatória desempenha um papel importante na criptografia. Os Planos em Blocos Incompletos Equilibrados (BIBD) são muito bem conhecidos como uma ferramenta para resolver problemas emergentes nesta área. No artigo publicado por Wang J. & Su R. em 2008, *Further Results on the Existence of Splitting BIBDs and Application to Authentication Codes* os autores mostram que as condições necessárias

para a existência de um BIBD $(v, u \times c, \lambda)$-*splitting* são $v \geq uc, \lambda(v-1) \equiv 0\ (mod\ c(u-1))$ e $\lambda v(v-1) \equiv (mod(c^2u(u-1)))$. Mostram, também, que as condições necessárias à existência de um BIBD $(v, 3 \times 3, \lambda)$-*splitting* são também possíveis, com possíveis exceções, quando $(c, \lambda) \in \{(55{,}1), (39{,}9k) : k = 1{,}2 \ldots\}$, $\lambda \equiv 0\ (mod\ 54)$ e $\lambda \equiv 0\ (mod\ 2)$. Os autores referem ainda a existência de um BIBD $(v, 3 \times 4{,}1)$ - *splitting* quando $v \equiv 1\ (mod\ 96)$. Com a aplicação destes, obtém-se uma nova classe de códigos de autenticação otimais.

Pinaki Sarkar & Amrita Saha apresentam um artigo, em 2011, intitulado: *Secure Communication Using Reed-Muller Codes and Partially Balanced Design in Wireless Sensor Network* na conferência IEEE Simpósio Internacional de Processamento Paralelo e Distribuído com aplicações Workshops - ISPAW (2011), no qual é feita referência às comunicações seguras através da utilização de códigos Reed-Muller e PBIBD, Planos em Blocos Incompletos Parcialmente Equilibrados, em Redes de Sensores Sem Fios e tendo em consideração que conetividade e comunicação são dois conceitos diferentes numa rede de sensores sem fios, (WSN). Estes autores propuseram um modelo para a conectividade de uma WSN utilizando códigos Reed Muller, no entanto no que diz respeito á comunicação, optaram por trabalhar com um modelo que utiliza parcialmente os PBIBD. Dois sistemas criptográficos podem agora ser aplicados para os dois modelos diferentes. Como resultado, a elasticidade da WSN é sensivelmente melhorada sem afetar a conetividade e escalabilidade do modelo de comunicação inicial. O estabelecimento de uma chave segura foi alcançado através da conversão de identificadores de nós públicos em informações privadas.

Ainda no âmbito da criptografia Barrera, et al., apresenta em 2013 o artigo, *Optical encryption and QR codes: Secure and noise-free information retrieval*, no qual desenvolvem o tema da encriptação ótica e exploram os Códigos QR na obtenção de dados de forma segura e sem ruídos na comunicação.

Francisco, C. & Oliveira, T. A., apresentam em 2014 o artigo, *BIBD, Hadamard Matrices and new technological devices: Applications to QR Codes*, ICNAAM 2014, International Conference of Numerical Analysis and Applied Mathematics 2014, Rhodes, Greece. Neste trabalho são abordadas as diferentes aplicações dos Códigos QR nas novas tecnologias, nomeadamente na Criptografia. Sendo a criptomoeda Bitcoin um exemplo disso, uma vez que se trata de uma moeda digital que usa um algoritmo

próprio tendo por base o uso dos Códigos QR. Apesar de existirem várias outras Criptomoedas deste tipo, esta é a mais utilizada.

Shah, D. & Shah, Y., apresentam em 2014 o artigo, *QR Code and its Security Issues*, no qual exploram os Códigos QR e os problemas de segurança inerentes aos mesmos. Sendo que um dos problemas mencionados se prende com o facto de ser possível a modificação dos dados contidos num Código QR. Os códigos Reed Solomon permitem não só detetar facilmente os erros mas também corrigi-los. Assim, é possível alterar pequenas quantidades de dados num Código QR sem que estas mesmas alterações sejam detetadas e uma vez que são imperceptíveis tornam-se num apetecível alvo para os piratas informáticos, mais vulgarmente denominados por *hackers*. Estes acedem e alteram os Códigos QR colocando em risco a informação dos dados neles armazenados, comprometendo seriamente toda a sua estrutura de segurança.

Zang, Y. et al., apresentam em 2015, uma técnica que permite combinar uma imagem, com um código QR, com o objetivo de o tornar esteticamente mais apelativo. Esta nova abordagem consiste em combinar a imagem com o código em duas etapas, uma a nível da área do código e outra a nível do pixel. Esta técnica apresenta três vantagens, aumenta a nível estético a aparência do Código QR, mantêm a mesma capacidade de correção de erros do código original e permite aproveitar toda a área do Código QR para combinar fotografias, desenhos e gráficos.

## Educação

Na área da Educação, Correia, H., usando como base o planeamento em blocos, apresenta em 2012, uma aplicação dos BIBDR com o objetivo de comparar cinco domínios do pensamento algébrico de uma amostra de alunos, tendo sido utilizado o *software* R para a análise dos dados da amostra. Verificaram-se diferenças significativas entre alguns dos domínios do pensamento algébrico, nomeadamente entre os domínios da Generalização da Aritmética e Tecnicismo Algébrico com os restantes domínios.

## Farmacologia

Samad, A. et. Al. apresenta em 2012 o artigo, *Bioequivalence Studies and Statistical Issues with High Variable Drugs,* no qual são desenvolvidos estudos estatísticos e de bioequivalência com HVDs.

## Genética

Silva, P. apresenta em 2009 um trabalho sobre aplicações dos planos em Blocos Incompletos Equilibrados na área da Genética, os *Diallel Crosses,* temática que possui hoje em dia um papel de grande relevo. O *Diallel Crosses* trata-se de um processo que pretende indagar as características genéticas de determinada população, para que se possa afirmar como sendo o mais eficaz e potente. A melhoria de linhas de plantas ou raças de animais cada vez mais refinadas e apuradas tem despertado continuamente o interesse dos geneticistas.

Oyekunle, M. et.al., apresentam em 2014 o artigo, *Genetic diversity of tropical early-maturing maize inbreds and their performance in hybrid combinations under drought and optimum growing conditions,* onde é avaliada e debatida a problemática do desenvolvimento de híbridos do milho, tendo em conta a diversidade genética e distância dentro de linhagens através do delineamento experimental.

## Informática

Rueda, D. et. Al. apresenta em 2011 o artigo, *A Memetic Algorithm for Designing Balanced Incomplete Blocks,* o qual explora a aplicação de algoritmos meméticos (MA) para o problema dos BIBD com resultados muito positivos.

Francisco, C. & Oliveira T. A., apresentam em 2014 o artigo, *BIBD, Hadamard Matrices and Combinatorial Analysis,* no SMTDA 2014, 3rd Stochastic Modeling Techniques and Data Analysis 2014, International Conference, em Lisboa, Portugal, desenvolvendo, o uso de estratégias de correção de erros uma vez que muitas das vezes

os Códigos QR, são expostos a condições adversas em que os dados que contêm podem ser perdidos, por isso, é muito importante que para limitar esse acontecimento a análise de risco não seja ignorada, tendo sido esta temática bastante discutida e ilustrada por meio da utilização de vários exemplos.

Francisco, C. & Oliveira, T. A., apresentam em 2014 o artigo, *Hadamard Matrices and new technological devices: applications to QR Codes*, na conferência SMSW 2014, Statistics and Mathematical Sciences 2014, Workshop in Honour of Professor João Tiago Mexia, na UBI - Universidade da Beira Interior, na Covilhã em Portugal, no qual é reforçada a ideia da ligação das matrizes de Hadamard aos BIBD e da utilização destas como base do desenvolvimento de códigos de correção de erros.

## Matemática e Estatística

Garcia, V. A., apresenta em 2011 um trabalho sobre os modelos de Planos em Blocos em geral e em particular os Planos em Blocos Incompletos Equilibrados com Repetições.
A análise estatística de um BIBD e de um BIBD com repetição de blocos (BIBDR) recorrendo a exemplos, bem como o explorar de algumas representações geométricas de planos com blocos, foi sucessivamente abordada ao longo deste trabalho.
No que respeita à dedução dos modelos gerais de análise, bem como na construção dos planos de estudo das possíveis estruturas e combinações de parâmetros, muitas questões ainda se levantam. Tanto na facilidade de aplicação prática como do ponto de vista económico é desejável a ocorrência da repetição de blocos, por outro lado em casos mais emblemáticos, nos quais unidades experimentais são perdidas por acidente, a existência de blocos repetidos é de extrema relevância.

Francisco, C.; Oliveira, T. A. & Oliveira, A. apresentam em 2014 um poster e o artigo, *Delineamento Experimental em blocos incompletos,* no ISCEE - Instituto Superior de Ciências Económicas e Empresariais no WSMC8 2014, 8th Workshop on Statistics Mathematics and Computation 2014, na Cidade da Praia, ilha de Santiago, Cabo Verde, onde é discutida a ligação das matrizes de Hadamard ao desenvolvimento de delineamentos experimentais com BIBD. Hoje em dia os delineamentos com BIBD encontram as aplicações mais diversas em vários campos da técnica, contudo é

importante explorar novas aplicações e melhorar as existentes, utilizando esta área do conhecimento como um novo desafio.

Francisco, C. & Oliveira, T. A., apresentam em 2014 o artigo, *Exploring links between Experimental Design and the Risk of Data Loss on QR Codes*, na Conferência CIAEEAR 2014, Internacional da Amazónia em Estatística Experimental e Análise de Risco 2014, na Universidade Federal do Amazonas, Manaus, Amazonas, Brasil, explorando o risco de perda de dados. De facto à medida que surgem novos resultados na evolução tecnológica, os Códigos QR são expostos a condições em que os seus dados podem ser perdidos, por isso, é muito importante para limitar esse risco, o uso de estratégias de correção de erros.

Monteiro, A. destaca no trabalho realizado em 2013, a importância do Planeamento de Experiências quando aplicado ao problema do ajuste dos parâmetros das meta-heurísticas e de que este é um problema essencial tanto na criação como na melhoria das meta-heurísticas. Uma meta-heurística é um método heurístico para resolver de forma genérica problemas de otimização. Os problemas de otimização combinatória têm, nos últimos anos atraído diversos investigadores não só pela sua aplicação prática, mas também pela sua dificuldade. Um crescente número de publicações tem sido desenvolvido por vários investigadores ao longo desta última década, no âmbito do ajuste dos parâmetros duma meta-heurística. Como as meta-heurísticas existentes já deram resposta à grande maioria dos problemas clássicos, a comunidade científica da área tem vindo a aperfeiçoar os modelos e técnicas existentes tendo em vista a obtenção de melhores resultados.

Balonin, N. A. & Seberry, J. apresentam em 2014 o artigo, *A review and new Symmetric Conference Matrices*, no qual desenvolvem o estudo das matrizes SCM (*Symmetric Conference Matrices*). Estas matrizes foram inicialmente apresentadas por Vitold Belevitch, o qual mostrou que estas permitem comunicações telefónicas sem perdas.

Yue, H. et. al. exploram no artigo publicado em 2014, as ligações entre os código binários de Hamming, os desenhos *t* combinatórios e as matrizes de Hadamard, obtendo neste seu trabalho resultados importantes.

# Capítulo 8

# Análise Estatística: Simulação de aplicações práticas possíveis em Medicina

## 8.1 – Introdução

Frequentemente surge a situação em que um investigador tem necessidade de comparar $v$ tratamentos. Para o efeito pretende aplicar-se a técnica de blocos como método de controlo sobre variáveis de prognóstico, mas o tamanho dos blocos desejável, *k* é menor do que *v*. O seguinte exemplo ilustra esta situação:

Cinco tratamentos irão ser comparados, utilizando blocos aleatórios, formados através do agrupamento dos pacientes, que integram o estudo mais perto uns dos outros, no tempo. O termo "*perto*" significa que não existe mais do que dois meses de diferença na data de início de integração dos pacientes no estudo. Apenas está prevista a entrada de dois pacientes por mês no estudo, para que o tamanho dos blocos $k = 3$ ou $k = 4$ seja menor do que o número de tratamentos $v = 5$.

Outro exemplo:

Pretende-se comparar seis pastas dentífricas utilizadas para tratamento preventivo de cáries, utilizando blocos aleatórios, considerando os quatro quadrantes da boca (superior e inferior esquerdo e superior e inferior direito) como a unidade experimental onde o tratamento será aplicado. O tamanho natural de cada bloco será $k = 4$, mas o número de tratamentos é $v = 6$.

## 8.2 – Delineamento experimental com BIBD

O delineamento experimental com BIBD é um delineamento por blocos onde o tamanho dos blocos $k$ é menor do que o número dos tratamentos $v$. Os BIBD são equilibrados devido ao facto de que $k$ tratamentos são administrados a cada bloco, cada tratamento aparece no mesmo número de blocos que qualquer outro tratamento e cada par de tratamentos aparece no mesmo número de blocos que quaisquer outro par de tratamentos. Um BIBD com tamanho de blocos $k$ e número de tratamentos $v$ pode ser obtido considerando as diferentes combinações (tuplos) de 1,2,…,$v$.

A Tabela 3 apresenta BIBDs até seis tratamentos:

| Tratamentos | Tamanho do Bloco | BIBDs |
|---|---|---|
| $v = 3$ | $k = 2$ | $(12), (13), (14)$ |
| $v = 4$ | $k = 2$ | $(12), (13), (14), (23), (24), (34)$ |
| $v = 4$ | $k = 3$ | $(123), (124), (134), (234)$ |
| $v = 5$ | $k = 2$ | $(12), (13), (14), (15), (23), (24), (25),$ $(34), (35), (45)$ |
| $v = 5$ | $k = 3$ | $(123), (124), (125), (134), (135), (145), (234),$ $(235), (245), (345)$ |
| $v = 5$ | $k = 4$ | $(1234), (1235), (1245), (1345), (2345)$ |
| $v = 6$ | $k = 2$ | $(12), (13), (14), (15), (16), (23), (24), (25), (26), (34),$ $(35), (36), (45), (46), (56)$ |
| $v = 6$ | $k = 3$ | $(123), (124), (136), (145), (156), (235), (246),$ $(256), (345), (346)$ |
| $v = 6$ | $k = 4$ | $(1234), (1235), (1236), (1245), (1246),$ $(1256), (1345),$ $(1346), (1356), (1456), (2345), (2346), (2356),$ $(2456), (3456)$ |
| $v = 6$ | $k = 5$ | $(12345), (12346), (12356), (12456), (13456), (23456)$ |

**Tabela 4** – Possíveis BIBD até seis tratamentos.
**Fonte:** Tabela parcial obtida de (Cochran, W. G. & Cox, G. M., 1957), Tabela 11.3.

Qualquer um destes delineamentos experimentais pode ser utilizado quando necessário e a sua utilização será ilustrada no exemplo prático que apresentarei mais adiante. Para uma lista de BIBDs com número de tratamentos até 28, (Cochran, W. G. & Cox, G. M., 1957).

## 8.3 – Descrição do exemplo prático

Na medicina, (Richards et al., 1994), no artigo *Interrater Reliability of the Unified Parkinson's Disease Rating Scale Motor Examination* (1994) apresentam um estudo de fiabilidade interexaminador, com o objetivo de avaliar se a escala UPDRS (unified parkinson's disease rating scale) pode ser utilizada com confiança na avaliação de um paciente. São utilizados BIBDs como base do delineamento experimental e análise deste estudo.

O exemplo prático que apresento foi inspirado neste estudo em particular, tratando-se de uma aplicação dos BIBD a um caso prático, através da utilização do *software* R para a análise estatística dos BIBD. A finalidade é salientar a importância da aplicação dos BIBD no delineamento experimental de ensaios clínicos.

Através de um exemplo prático pretende-se demonstrar a utilização dos BIBD numa situação de análise de um ensaio clínico. Apesar do mesmo ser construído com base em dados fictícios este vai tornar possível uma melhor compreensão de como utilizar blocos incompletos equilibrados numa situação de delineamento experimental.

De seguida enuncia-se o estudo que se deseja analisar:

Pretende-se comparar seis neurologistas, num estudo de fiabilidade interexaminador. No estudo participarão dez pacientes que sofrem da doença de Parkinson. Cada paciente inscrito no estudo será examinado, de forma separada e independente, por vários neurologistas. Cada paciente define um bloco. Cada paciente não tolera mais de três exames. Com base nas condições enunciadas verifica-se que, se os pacientes não toleram mais do que três exames então o tamanho máximo do bloco $k = 3$ é menor do que o número de examinadores, $v = 6$.

Outras condições do estudo são descritas a seguir:

Participarão do estudo dez pacientes e cada um destes será examinado por três neurologistas.

Cada um dos seis neurologistas examinará cinco pacientes.

Cada par de examinadores examina dois pacientes.

Estas três condições definem o estudo como sendo um BIBD.

Quando existe a necessidade de comparar cada par de médicos (ou de tratamentos), com a mesma precisão, o delineamento experimental com blocos incompletos equilibrados, BIBD, proposto por (Yates, F., 1936), é o método mais apropriado para realizar o estudo.

Neste exemplo utiliza-se o BIBD $(v, b, r, k, \lambda) = (6,10,5,3,2)$, onde $v$ denota o número de tratamentos ou variedades, neste caso $v$ é o número de neurologistas que se pretende comparar, $b$ é o número de blocos a que os tratamentos serão aplicados, neste caso temos dez pacientes, $r$ é o número de pacientes examinado por cada médico neurologista (examinador), $k$ é o tamanho do bloco ou o número de tratamentos que pode ser aplicado a cada bloco, neste caso $k = 3$ pois os pacientes não toleram mais do que três exames, e $\lambda$ é o número de blocos onde cada par de variedades ocorre, neste caso $\lambda$ é o número de pacientes examinado por cada par de examinadores.

As condições necessárias à existência de um BIBD com estes parâmetros são, como visto anteriormente:

$vr = bk$ ; $v \leq b$ e $\lambda(v-1) = r(k-1)$.

A Tabela 4 de dados reflete o resultado dos exames efetuados aos pacientes:

| | Examinador | | | | | | |
|---|---|---|---|---|---|---|---|
| Paciente | 1 | 2 | 3 | 4 | 5 | 6 | Média |
| 1 | 66 | 93 | 66 | | | | 75,00 |
| 2 | 20 | 20 | | 7 | | | 15,66 |
| 3 | 46 | | 80 | | | 60 | 62,00 |
| 4 | 20 | | | 53 | 33 | | 35,33 |
| 5 | 133 | | | | 172 | 133 | 146,00 |
| 6 | | 133 | 93 | | 133 | | 119,66 |
| 7 | | 33 | | 53 | | 93 | 59,66 |
| 8 | | 93 | | | 119 | 100 | 104,00 |
| 9 | | | 80 | 113 | 80 | | 91,00 |
| 10 | | | 119 | 126 | | 86 | 110,33 |
| Média | 57 | 74,4 | 87,6 | 70,4 | 107,4 | 94,4 | 81,86 |

**Tabela 5** – Resultados dos exames efetuados a dez pacientes.

Cada valor desta tabela representa a pontuação atribuída pelo examinador ao paciente indicado. Estes valores que foram utilizados no exemplo virtual estão de acordo com o que se passaria numa eventual situação real, pois são provenientes da escala *Unified Parkinson's Disease Rating Scale* (UPDRS). Esta escala foi desenvolvida como uma tentativa de combinar elementos de diversas outras escalas que existiam anteriormente e com isso produzir uma ferramenta eficaz e flexível para monitorar o impacto da doença de Parkinson e o grau de incapacidade provocado por esta doença, num paciente. A escala foi introduzida em 1987 e desde então tem sido atualizada por especialistas da *Movement Disorder Society*.

Pode encontrar-se maior detalhe sobre esta escala no seguinte site: http://www.epda.eu.com/en/parkinsons/in-depth/parkinsonsdisease/rating-scales/updrs/ .

A pontuação desta escala varia desde 0 (paciente não apresenta incapacidade) até 199 (paciente que apresenta incapacidade severa).

A distribuição dos resultados pelas colunas da tabela segue o BIBD com $v = 6$ ; $k = 3 : (123), (124), (136), (145), (156), (235), (246), (256), (345), (346)$, descrito na Tabela 4.

Outra opção consiste na utilização do *software* R para criar o BIBD. Para tal utiliza-se o comando > *find.BIB(6, 10, 3)* e o R responde com o conjunto dos blocos, que são neste caso coerentes com a tabela anterior, mas que poderiam ser outros também válidos, Figura 18:

```
> find.BIB(6,10,3)
      [,1] [,2] [,3]
 [1,]    1    4    5
 [2,]    1    2    3
 [3,]    1    2    4
 [4,]    3    4    6
 [5,]    3    4    5
 [6,]    2    4    6
 [7,]    1    3    6
 [8,]    1    5    6
 [9,]    2    5    6
[10,]    2    3    5
```

**Figura 18** – Blocos para o BIBD (6,10,5,3,2).

### 8.4 – Análise de dados de um BIBD

O modelo de análise para um BIBD é descrito a seguir:

Seja $X_{ij}$ o valor atribuído a um paciente no bloco $i$, o qual recebeu o tratamento $j$. Então $X_{ij}$ pode ser descrito como:

$$X_{ij} = \mu + s_i + \alpha_j + \epsilon_{ij},$$

onde μ é a média global de todas as observações, $s_i$ é um efeito aleatório devido ao bloco $i$, com média zero e variância $\sigma_s^2$, $\alpha_j$ é o efeito devido ao tratamento $j$ sujeito a $\sum_{j=1}^{v} \alpha_j = 0$ e $\epsilon_{ij}$ são erros aleatórios independentes e identicamente distribuídos, com média zero, variância $\sigma_\epsilon^2$ e com efeitos aleatórios $s_i$'s.

Para verificar se há diferenças estatisticamente significativas no efeito dos tratamentos serão testadas as seguintes hipóteses:

$H_0: \tau_1 = \tau_2 = \cdots = \tau_a$ *versus* $H_1: \tau_i \neq \exists_{i,j:} \tau_i \neq \tau_j; i \neq j (i, j = 1, \ldots a)$ para pelo menos um $i$.

A estatística de teste é dada por:

$$F = \frac{TMS(EB)}{RMS} \sim F_{v-1, rv-b-v+1, \alpha}$$

onde a razão $F$ é o valor observado da estatística de teste F da distribuição F de Fisher com $v - 1$ e $rv - b - v + 1$ graus de liberdade.

A regra de decisão é dada por:

Se $F > F_{v-1, rv-b-v+1, \alpha}$ deve-se rejeitar $H_0$, ao nível de significância α.

A análise efetuada designa-se análise intra-bloco porque as diferenças entre blocos são eliminadas e porque todos os contrastes no efeito dos tratamentos podem ser expressos como comparação entre observações no mesmo bloco.

O valor-*p* representa a probabilidade do efeito, ou da diferença, observada entre os tratamentos se dever apenas ao acaso, e não aos fatores que estão a ser estudados.

Como exemplo, um valor-*p* de 0,3 significa que, a probabilidade da diferença entre as médias se dever ao acaso, e não ao efeito dos tratamentos, é de 30%. Ou seja, se o investigador afirmar que as diferenças entre as médias ocorreram por causa dos tratamentos, ele tem 30% de hipótese de estar enganado.

O valor-p pode variar entre 0 e 1. Na maioria dos estudos, admite-se um valor crítico de *p* menor ou igual a 0,05, ou seja, assume-se como margem de segurança 5% de probabilidade de erro, ou seja 95% de probabilidade de estar certo. Assim com $\alpha = 0.05$, se o valor-*p* for inferior a 0.05, ou seja a 5%, a hipótese nula é rejeitada.

**8.5 – Análise do efeito dos tratamentos**

Uma estimativa aproximada para $\alpha_j$ é definida como:

$$\hat{\alpha}_j = \bar{X}_{.j} - \bar{X} \ldots$$

A estimativa aproximada não é enviesada, ou seja é centrada, mas está sujeita a uma excessiva variação aleatória devido à sua variância ser afetada por $\sigma_s^2$ e $\sigma_\epsilon^2$.

Uma estimativa intuitivamente mais razoável é dada por $\bar{X}_{.j} - M_j$, onde $M_j$ é a média das respostas referente apenas aos blocos que envolvem o tratamento $j$.

**Definição:**

Sejam $jl, l = 1, \dots, r$ os blocos aos quais se aplicou o tratamento $j$ e seja $\bar{X}_{jl\cdot}$ a média no bloco $jl$. Então,

$M_j = \frac{1}{r}\sum_{l=1}^{r} \bar{X}_{jl\cdot}$,

e tem-se que,

$$\bar{X}_{.j} - M_j = \frac{1}{r}\sum_{l=1}^{r}\left(X_{jlj} - \bar{X}_{jl\cdot}\right).$$

Assim, pode depreender-se que:

$$E\left(\bar{X}_{.j} - M_j\right) = \frac{v(k-1)}{k(v-1)}\alpha_j$$

**Definição:**

Seja $EFF = \frac{v(k-1)}{k(v-1)}$. Este fator, EFF é chamado fator de eficiência do delineamento. Então uma estimativa não enviesada de $\alpha_j$, estimador dos mínimos quadrados, será dada por:

$a_j = \frac{1}{EFF}(\bar{X}_{.j} - M_j)$,

e pode-se verificar que:

$Var(a_j) = \frac{v-1}{v}\frac{\sigma_\epsilon^2}{rEFF}$.

A soma dos quadrados (contribuição do efeito dos tratamentos para a soma dos quadrados total) é dada por:

$$TSS(EB) = rEFF \sum_{j=1}^{v} a_j^2.$$

A tabela ANOVA para a análise do efeito dos tratamentos, Tabela 5:

| Fonte de Variação | Graus de Liberdade | Soma de Quadrados | Quadrados Médios | E(MS) | F |
|---|---|---|---|---|---|
| Block(IT) | $b-1$ | $k\sum(\bar{X}_{i.}-\bar{X}_{..})^2$ | BMS(IT) | $\sigma_\epsilon^2 + k\sigma_s^2 + \frac{r-\lambda}{k(b-1)}\sum \alpha_j^2$ | $\frac{k\sum(\bar{X}_{i.}-\bar{X}_{..})}{RMS}$ |
| Tmt(EB) | $v-1$ | $rEFF\sum_{j=1}^{v} a_j^2$ | TMS(EB) | $\sigma_\epsilon^2 + \frac{rEFF}{v-1}\sum \alpha_j^2$ | $\frac{TMS(EB)}{RMS}$ |
| Res. | $rv-b-v+1$ | Por subtração | RMS | $\sigma_\epsilon^2$ | |
| Total | $rv-1$ | $\sum\sum(X_{ij}-\bar{X}_{..})^2$ | | | |

**Tabela 6** – ANOVA para a análise dos efeitos dos tratamentos.

Onde IT: Ignorando tratamentos; EB: Eliminando o efeito dos blocos.

Através dos quadrados médios da tabela ANOVA, deve ser notado que o TMS(EB) providencia uma medida válida para o efeito dos tratamentos e BMS(IT) não providencia uma medida válida dos efeitos dos blocos. Para além disso, este mede apenas parcialmente o efeito dos tratamentos. A significância do efeito dos tratamentos é testada através da razão F (razão do modelo pelo seu erro):

$$F = \frac{TMS(EB)}{RMS}.$$

Este valor será comparado com $F_{v-1,rv-b-v+1,\alpha}$ para um teste ao nível de significância $\alpha$.

Serão testadas as seguintes hipóteses:

$H_0$: $\tau_1 = \tau_2 = \cdots = \tau_a$ versus $H_1$: $\tau_i \neq 0$ para pelo menos um $i$.

A regra de decisão é dada por:

Se $F > F_{v-1,rv-b-v+1,\alpha}$ deve-se rejeitar $H_0$, ao nível de significância $\alpha$.

## 8.6 – Comparação Múltipla

Comparações múltiplas são obtidas através de contrastes sob a forma:

$$C = \sum_{j=1}^{v} c_j a_j \ , \sum_{j=1}^{v} c_j = 0 \ .$$

A variância estimada de $C$ será:

$$Var(C) = \frac{RMS}{rEFF} \sum_{j=1}^{v} c_j^2 .$$

A estatística de teste é dada por:

$$L = \frac{C}{\sqrt{Var(C)}} ,$$

a qual segue, sob $H_0$, uma distribuição $t$ de Student com graus de liberdade $rv - b - v + 1$ .

## 8.7 – Análise do efeito dos blocos em planos simétricos

Uma soma de quadrados adequada deverá medir, para além dos efeitos dos tratamentos, os efeitos dos blocos. A soma de quadrados desejada para os efeitos dos blocos pode ser obtida da mesma forma que a soma de quadrados para os efeitos dos tratamentos.

Vamos estudar a análise do efeito dos blocos no caso particular dos planos simétricos, onde, tal como o nome indica, existe uma estrutura simétrica entre blocos e tratamentos. Assim, na forma matemática os tratamentos podem ser considerados como sendo blocos, e os blocos como sendo tratamentos.

Quando se troca os papéis entre blocos e tratamentos, os seguintes parâmetros também invertem os seus papéis:

r <=> k ; $b$ <=> $v$

$$\frac{1}{v-1}\sum \alpha_j^2 \ <=> \ \sigma_s^2 \ .$$

Utilizando a simetria descrita acima, define-se:

$$\overline{EFF} = \frac{b(r-1)}{r(b-1)}, \quad b_i = \frac{1}{\overline{EFF}}(\bar{X}_{i.} - M_i'),$$

onde os $M_i'$'s são similarmente definidos como $M_j$'s.

Através do argumento de simetria forma-se a tabela ANOVA, Tabela 6. Esta tabela é utilizada para analisar os efeitos dos blocos.

| Fonte de Variação | Graus de Liberdade | Soma de Quadrados | Quadrados Médios | E(MS) |
|---|---|---|---|---|
| Block(ET) | $b-1$ | $k\overline{EFF}\sum_{i=1}^{b} b_j^2$ | BMS(ET) | $\sigma_\epsilon^2 + k\overline{EFF}\sigma_s^2$ |
| Tmt(IB) | $v-1$ | $r\sum(\bar{X}_{.j} - \bar{X}_{..})^2$ | TMS(IB) | $\sigma_\epsilon^2 + \frac{r}{v-1}\sum \alpha_j^2 + \frac{v-k}{v-1}\sigma_s^2$ |
| Res. | $rv-b-v+1$ | Por subtracção | RMS | $\sigma_\epsilon^2$ |
| Total | $rv-1$ | $\sum\sum(X_{ij} - \bar{X}_{..})^2$ | | |

**Tabela 7** – ANOVA para análise dos efeitos dos blocos.

A significância do efeito dos blocos é testada através da razão F (razão do modelo pelo seu erro) :

$$F = \frac{BMS(ET)}{RMS}.$$

Este valor será comparado com $F_{v-1,rv-b-v+1,\alpha}$ para um teste ao nível de significância $\alpha$.

Serão testadas as seguintes hipóteses:

$H_0$: $\tau_1 = \tau_2 = \cdots \tau_a$ versus $H_1$: $\tau_i \neq 0$ para pelo menos um $i$.

A regra de decisão é dada por:

Se $F > F_{v-1,rv-b-v+1,\alpha}$ deve rejeitar-se $H_0$ para o nível de significância $\alpha$.

## 8.8 – A abordagem do modelo linear

A resposta X num BIBD é expressa num outro sistema linear, com reparametrização, da seguinte forma:

$$X = \mu + \sum_{i=2}^{b} \gamma_i b_i + \sum_{j=2}^{v} \beta_j t_j + \epsilon \,,$$

onde:

$$b_i = \begin{cases} 1, se\ bloco\ i \\ 0, caso\ contrário, i = 2, \dots, b \end{cases}$$

$$t_j = \begin{cases} 1, se\ tratamento\ j \\ 0, caso\ contrário, j = 2, \dots, v \end{cases} .$$

Os testes de hipóteses para os efeitos dos tratamentos e para os efeitos dos blocos, são equivalentes ao teste para $H_0: \beta_2 = \cdots = \beta_v = 0$ e $H_0 : \gamma_2 = \cdots = \gamma_b = 0$, respetivamente.

A comparação múltipla sobre os efeitos do tratamento resume-se ao teste linear correspondente, dos parâmetros $\beta$.

As duas tabelas ANOVA podem ser obtidas ajustando o modelo duas vezes, utilizando a função do R, *lm*, a qual é utilizada para ajustar modelos lineares**.** Este processo é realizado em duas etapas. Primeiro coloca-se o fator dos blocos antes do fator dos tratamentos na especificação da fórmula para obter a tabela ANOVA para inferência sobre os efeitos dos tratamentos, e de seguida realiza-se a segunda etapa, coloca-se o fator dos tratamentos antes do fator dos blocos, obtendo-se desta forma a tabela ANOVA para inferência sobre os efeitos dos blocos.

## 8.9 – Aplicação ao estudo de fiabilidade interexaminador

### 8.9.1 – Fiabilidade da medida

A fiabilidade da medida refere-se à qualidade dos dados, ou seja, se os dados obtidos são ou não dignos de confiança.

Uma medida de uma característica de um paciente pode ser expressa como:

$$X_i = S_i + \epsilon_i \, ,$$

onde $S_i$ é o valor real da característica, o qual segue uma distribuição com média $\mu$ e variância $\sigma_s^2$ e $\epsilon_i$ é um erro aleatório de medição, distribuído com média zero e variância $\sigma_\epsilon^2$.

O coeficiente de fiabilidade é definido como:

$$CF = \frac{\sigma_s^2}{\sigma_X^2} .$$

No caso simples apresentado acima, $\sigma_X^2 = \sigma_s^2 + \sigma_\epsilon^2$ .

A fiabilidade é a aptidão para um resultado demonstrar consistência, ou seja que esteja livre de erros de medição, em medidas repetidas. Esta qualidade de medição pode ser explicada em termos de valores observados, valores verdadeiros e valores do erro cometido. A teoria da fiabilidade assume que qualquer medição numa escala contínua contém uma componente de erro, ou seja um erro de medição que interessa estimar.
O conceito de correlação intraclasse foi introduzido por (Fisher, R. A., 1925). A medida de fiabilidade mais utilizada é o coeficiente de correlação intraclasse, o qual é utilizado quando as variáveis do estudo são contínuas. O coeficiente de correlação intraclasse é uma medida da fiabilidade dos observadores. Esta medida é definida como a razão da variância entre as unidades em análise e a variância total. Estas variâncias são derivadas da análise de variância, ANOVA, na qual se assume que os observadores são obtidos aleatoriamente de uma população maior de observadores. Este coeficiente é sempre positivo e não vem expresso em qualquer unidade de medida. Os valores resultantes para este coeficiente variam entre 0 e 1, com os valores próximos de 1 a indicarem uma

fiabilidade elevada. Quando o valor é igual a 0 o estudo não é reprodutível, ou seja, existe uma grande variabilidade intra-observador, mas não há variabilidade inter-observador. No caso do valor obtido ser igual a 1, o estudo é reprodutível ao máximo, ou seja, não há variabilidade intra-observador, mas há uma grande variabilidade inter-observador. Para interpretação dos valores do coeficiente de correlação (fiabilidade) utiliza-se a escala de valores proposta por (Menz et al., 2004), a qual se apresenta na Tabela 7:

| Valor do Coeficiente (CF) | Interpretação do resultado |
|---|---|
| $0.4 \leq CF < 0.75$ | Moderado / Satisfatório |
| $CF < 0.4$ | Pobre |
| $CF \geq 0.75$ | Excelente |

**Tabela 8** – Interpretação dos valores do coeficiente de correlação

Valores acima de 0,75 mostram excelente fiabilidade; valores entre 0,40 - 0,75, fiabilidade moderada/satisfatória e valores abaixo de 0,40 mostram pouca fiabilidade.

### 8.9.2 – Fiabilidade da medida dada por diferentes examinadores

A fiabilidade inter-examinador surge quando a medição dos pacientes é efetuada por diferentes examinadores ou avaliadores. Supondo que a medição de cada paciente é efetuada por um examinador designado aleatoriamente a partir de um conjunto de $v$ examinadores, a medida obtida sobre o paciente $i$ efectuada pelo examinador $j$ pode ser expressa como:

$$X_{ij} = S_i + \alpha_j + \epsilon_{ij} .$$

Neste caso,

$$\sigma_X^2 = \sigma_s^2 + \frac{1}{v}\sum_{j=1}^{v} \alpha_j^2 + \sigma_\epsilon^2 ,$$

e o coeficiente de fiabilidade intraclasse é dado por:

$$CF = \frac{\sigma_s^2}{\sigma_s^2 + \frac{1}{v}\sum_{j=1}^{v} \alpha_j^2 + \sigma_\epsilon^2}.$$

### 8.9.3 – Estimação do coeficiente de fiabilidade

Estimativa de $\sigma_\epsilon^2$ :

Um estimador não enviesado para $\sigma_\epsilon^2$ é dado por:

$$\hat{\sigma}_\epsilon^2 = RMS\,.$$

Estimativa de $v^2 = \frac{1}{v}\sum_{j=1}^{v} \alpha_j^2$ :

Através da tabela ANOVA para inferência sobre os efeitos dos tratamentos, é possível obter um estimador não enviesado para $v$. Este é definido da seguinte forma:

$$\hat{v}^2 = \frac{v-1}{rEFF}\frac{TMS(EB) - RMS}{v}.$$

Estimativa de $\sigma_s^2$ :

Através da tabela ANOVA para inferência sobre os efeitos dos blocos, é possível obter um estimador não enviesado para $\sigma_s^2$. Este é definido da seguinte forma:

$$\hat{\sigma}_s^2 = \frac{1}{k\overline{EFF}}(BMS(ET) - RMS)\,.$$

Estimativa do coeficiente de fiabilidade:

O coeficiente de fiabilidade, $CF$, é estimado através de:

$$CF = \frac{\hat{\sigma}_s^2}{\hat{\sigma}_s^2 + \hat{v}^2 + \hat{\sigma}_\epsilon^2}.$$

## 8.10 – Análise do exemplo virtual

Para a análise dos dados do exemplo, irá ser utilizado o s*oftware* R, presentemente na sua versão 3.1.2. Começa-se por introduzir no R todos os dados do problema que queremos estudar. Para tal constroem-se variáveis, do tipo vetor, com os dados do problema, utilizando o comando:

$$valores = c(66,93,66,20,20,7,46,80,60,20,53,33,133,172,133,133,93,133,$$

$$33,53,93,93,119,100,80,113,80,119,126,86).$$

Este comando permite introduzir na variável $valores$ os valores da pontuação atribuída pelos examinadores aos pacientes.

De seguida faz-se o mesmo para o conjunto de valores que descreve o BIBD a ser utilizado:

$$examinador = c(1,2,3,1,2,4,1,3,6,1,4,5,1,5,6,2,3,5,2,4,6,2,5,6,3,4,5,3,4,6)$$

O R permite a utilização de variáveis qualitativas ou categóricas. No R, as variáveis categóricas são definidas usando o comando $factor$. Utilizando o comando abaixo, transforma-se a variável $examinador$ do tipo vector, numa variável categórica:

$$examinador = factor(examinador)$$

O grupo de dez pacientes pode ser representado por um vetor que contém os números de 1 a 10. Isto é conseguido no R com o comando $1{:}\,10$, como se pode verificar:

```
> 1:10
 [1]  1  2  3  4  5  6  7  8  9 10
```

**Figura 19** – Resposta do R, mostra o conteúdo de um vetor com dez entradas.

Em seguida representa-se o facto de cada um dos dez pacientes ser examinado três vezes. Para isso realiza-se o produto de Kronecker do conjunto anterior com os números de 1 a 10, pelo vetor que contém três elementos unitários $c(1,1,1)$. O resultado do R é mostrado a seguir:

```
> kronecker(1:10,c(1,1,1))
 [1]  1  1  1  2  2  2  3  3  3  4  4  4  5  5  5  6  6  6  7  7  7  8  8  8  9  9  9 10 10 10
```

**Figura 20** – Resposta do R, mostra o resultado da execução do produto de Kronecker do vetor com dez entradas pelo vetor unitário (1,1,1) .

Este resultado constituirá a variável categórica $paciente$, definida com recurso ao comando:

$$paciente = factor(kronecker(1{:}\,10, c(1,1,1))).$$

Antes de se solicitar ao R para criar as tabelas ANOVA, torna-se útil definir os contrastes que se vão utilizar. Para esse efeito introduz-se no R o seguinte comando:

$$options(contrasts = c(\text{contr.treatment,contr.poly})).$$

Uma análise de variância também pode ser expressa como um modelo linear. Neste utiliza-se um fator como variável independente para modelar uma variável de resposta. Para construir um modelo linear no R utiliza-se a função $lm$:

$$lm.ajuste1 = lm(valores{\sim}paciente + examinador).$$

A expressão anterior representa um modelo típico $resposta{\sim}termos$ onde $resposta$ é o vetor dos valores da pontuação atribuída pelos examinadores e os $termos$ são uma série de variáveis que em conjunto especificam um preditor linear para a $resposta$. Neste caso $paciente + examinador$ indica todos os termos do primeiro, juntamente com todos os termos do segundo com remoção de quaisquer termos duplicados que possam existir.

O resultado é colocado na variável $lm.ajuste1$, com a qual é então construída a tabela ANOVA, com recurso ao comando $anova(lm.ajuste1)$.

A Figura 21 ilustra a introdução dos vários comandos anteriores, no R, bem como a tabela ANOVA produzida, para a inferência sobre o efeito dos tratamentos (exames feitos pelos examinadores).

```
> valores = c(66,93,66,20,20,7,46,80,60,20,53,33,133,172,133,133,93,133,33,53,
+             93,93,119,100,80,113,80,119,126,86)
> examinador = c(1,2,3,1,2,4,1,3,6,1,4,5,1,5,6,2,3,5,2,4,6,2,5,6,3,4,5,3,4,6)
> examinador = factor(examinador)
> paciente = factor(kronecker(1:10,c(1,1,1)))
> options(contrasts=c("contr.treatment" ,"contr.poly" ))
> lm.ajuste1 = lm(valores~paciente+examinador)
> anova(lm.ajuste1)
Analysis of Variance Table

Response: valores
           Df Sum Sq Mean Sq F value    Pr(>F)
paciente    9  43224  4802.7  11.739 2.638e-05 ***
examinador  5   1547   309.3   0.756    0.5948
Residuals  15   6137   409.1
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
>
```

**Figura 21** – Resposta do R, ANOVA para a inferência sobre o efeito dos tratamentos.

Pretende-se testar as seguintes hipóteses:

$H_0$ : não existe diferença entre examinadores vs $H_1$ : pelo menos um examinador é diferente.

O valor observado da estatística de teste F, será comparado com o valor crítico da distribuição F de Fisher:

0.756 será comparado com F(5,15,0.05) = 2.90

O valor anterior pode ser obtido com o seguinte comando do R:

```
> qf(.95, df1=5, df2=15)
[1] 2.901295
>
```

**Figura 22** – Resposta do R à consulta do valor da distribuição F de Fisher

Como 0.756 é inferior a 2.90 não se rejeita a hipótese nula, logo constata-se que a um nível de significância de 5% não existe diferença entre examinadores. O valor-$p$ confirma que a probabilidade do resultado ser devida ao acaso é pequena.

Em seguida constrói-se um segundo modelo linear, no qual os valores agora terão como preditor linear o conjunto $examinador + paciente$, ou seja utiliza-se todos os termos da variável $examinador$, juntamente com todos os termos da variável $paciente$ com remoção dos duplicados, como termos preditores dos valores da variável $resposta$. O comando para a construção deste segundo modelo no R é:

$$lm.ajuste2 = lm(valores \sim examinador + paciente)$$

Deste produz-se uma segunda tabela ANOVA, para inferência sobre o efeito dos blocos (pacientes). A figura abaixo ilustra a construção do segundo modelo linear no R, bem como a segunda tabela ANOVA produzida, utilizando o comando $anova(lm.ajuste2)$:

```
> lm.ajuste2=lm(valores~examinador+paciente)
> anova(lm.ajuste2)
Analysis of Variance Table

Response: valores
           Df Sum Sq Mean Sq F value    Pr(>F)
examinador  5   8237  1647.5  4.0269    0.0162 *
paciente    9  36533  4059.2  9.9218 7.35e-05 ***
Residuals  15   6137   409.1
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
>
```

**Figura 23** – Resposta do R, sobre o efeito dos blocos (pacientes).

Pretende-se testar as seguintes hipóteses:

$H_0$ não existe diferença entre pacientes vs $H_1$ existe pelo menos um paciente diferente.

O valor observado da estatística de teste F, será comparado com o valor crítico da distribuição F de Fisher:

9.9218 será comparado com F(9,15,0.05) = 2.587626

O valor anterior pode ser obtido com o seguinte comando do R:

```
> qf(.95, df1=9, df2=15)
[1] 2.587626
>
```

**Figura 24** – Resposta do R à consulta do valor da distribuição F de Fisher

Como 9.9218 é superior a 2.5876 rejeita-se a hipótese nula, logo constata-se que a um nível de significância de 5% existem diferenças entre os pacientes. O valor-*p* confirma que a probabilidade do resultado ser devida ao acaso é pequena.

### 8.10.1 – Cálculo do coeficiente de fiabilidade

Tem-se que:

$$\mathrm{EFF} = \frac{\mathrm{v(k-1)}}{\mathrm{k(v-1)}} = \frac{6\times(3-1)}{3\times(6-1)} = \frac{4}{5},$$

$$\overline{EFF} = \frac{b(r-1)}{r(b-1)} = \frac{10\times(5-1)}{5\times(10-1)} = \frac{8}{9},$$

$$\hat{v}^2 = \frac{v-1}{rEFF}\frac{TMS(EB)-RMS}{v} = \frac{(6-1)(309.3-409.1)}{6\times5\times\frac{4}{5}} = -20.7917\,,$$

o valor estimado para $\hat{v}^2$ é negativo, porém o parâmetro que este estima, $\frac{1}{v}\sum_{j=1}^{v}\alpha_j^2$ ou seja $\sum\frac{\alpha_j^2}{v}$, não pode nunca ser negativo,

$$\hat{\sigma}_s^2 = \frac{1}{k\overline{EFF}}(BMS(ET)-RMS) = \frac{1}{3\times\frac{8}{9}}(4059.2-409.1) = 1368.79,$$

de onde se obtém o coeficiente, estimado, de fiabilidade intraclasse:

$$\widehat{CF} = \frac{\sigma_s^2}{\sigma_s^2+\hat{v}^2+RMS} = \frac{1368.79}{1368.79+(-20.7917)+409.1} = 0.7790$$

### 8.10.2 – Discussão dos resultados

Sempre que se utilizam seres humanos como parte de um procedimento de medição, torna-se necessário avaliar se os resultados obtidos são confiáveis ou consistentes.

No exemplo anterior isto é conseguido através de um estudo de fiabilidade inter-examinador. O valor obtido, para o coeficiente de fiabilidade, 0.7790, o que de acordo com a escala de valores proposta por (Menz et al., 2004), indica uma excelente fiabilidade. Conclui-se que existe boa consistência entre os resultados apresentados pelos diferentes examinadores, e consequentemente na utilização da escala UPDRS na avaliação do impacto da doença de Parkinson nos pacientes observados.

# Capítulo 9

# Considerações e perspetivas de investigação futura

Neste trabalho procurámos abordar e explorar o Delineamento Experimental em blocos incompletos através do estudo de casos particulares e abordando ligações com temáticas atuais.
Hoje em dia os investigadores das diferentes áreas têm dado o seu contributo para o desenvolvimento das aplicações dos BIBD, o que se tem revelado de extrema importância para a uma evolução global científico-tecnológica.

Tal como mencionado no capítulo 7, várias abordagens recentes estão relacionadas com ensaios clínicos, sendo que se dedica especial atenção a esta temática na aplicação prática virtual apresentada no capítulo 8.

Determinámos uma lista de possíveis parâmetros para os BIBDR com $k = 7$. Propõe-se como trabalho futuro o desenvolvimento da lista de parâmetros para os BIBDR com outros valores de *k*.

Numa pesquisa das aplicações em outras áreas da Ciência interessámo-nos por investigar o historial de aplicações dos BIBD no âmbito dos Qr Codes, visto ser um tema muito interessante e que recentemente integra a realidade social.

No decorrer deste estudo muitas e interessantes questões ficaram em aberto, que ambicionamos continuar a aprofundar.

Destacam-se:

- Delineamento Experimental em blocos incompletos equilibrados: Análise de variância e continuação do estudo de modelos, estruturas e parâmetros dos PBIE;

- Investigação de casos particulares: Planos com blocos repetidos, Planos com blocos de diferentes dimensões e Planos com número de réplicas variável;

- Estabelecimento de metas e objetivos para aplicações a desenvolver;

- Pesquisa bibliográfica e em ambiente *online* de literatura relevante para o desenvolvimento de aplicações a casos reais; desenvolvimento de *software* para casos particulares;

- Continuar a explorar as vantagens de aplicação dos BIBD nos Códigos QR e em novas áreas no domínio das Tecnologias de Informação e Comunicação (TICs).

## Referências Bibliográficas


Balonin, N. A. & Seberry, J. (2014): *A review and new Symmetric Conference Matrices.* Informatsionno-upravliaiushchie sistemy, 71 (4), 2-7. Disponível em: http://ro.uow.edu.au/eispapers/2748/. Acesso em 10/12/2014.

Barrera, J. F.; Mira, A. & Torroba, R. (2013): *Optical encryption na QR codes: Secure and noise-free information retrieval*. The International Online Journal of Optics. Editor: Andrew M. Weiner Vol. 21, Iss. 5 – Mar. 11, 5373-5378. Disponível em: http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-21-5-5373. Acesso em 09/08/2014.

Baumert, L.; Golomb, S. W. & Marshall Hall, Jr. (1962): *Discovery of an Hadamard matrix of order 92*. Bull. Amer. Math. Soc. 68, no. 3, 237--238.

Cochran, W. G. & Cox, G. M. (1957): *Experimental Designs.* 2nd edition John Wiley and Sons, New York.

Correia, H. (2012): Planeamento *de Experiências: Modelos e desafios dos Planos em Blocos Incompletos*. Dissertação de Mestrado em Estatística, Matemática e Computação, área de especialização Estatística Computacional. Universidade Aberta.

EPDA, European Parkinson's Disease Association (1987): *unified Parkinson's Disease Rating Scale (UPDRS)*. Disponível em: http://www.epda.eu.com/en/parkinsons/in-depth/parkinsonsdisease/rating-scales/updrs/. Acesso em 29/03/2014.

Fisher, R. A. (1925): *Statistical methods for research workers*. New York, Hafner Press.

Foody, W. & Hedayat, A. (1977): *On theory and applications of BIB Designs with repeated blocks.* The Annals of Statistics, 5 (5): 932 - 945.

Francisco, C.; Oliveira, T. A. & Oliveira, A. (2014): *BIBD, Delineamento Experimental em blocos incompletos*, in Proceedings of WSMC8 2014, 8th Workshop on Statistics Mathematics and Computation. ISCEE - Instituto Superior de Ciências Económicas e Empresariais, Cidade da Praia, ilha de Santiago, Cabo Verde, 12 a 15 Março 2014. Disponível em: https://sites.google.com/site/wsmc2014cv/ . Acesso em 21/02/2014.

Francisco, C. & Oliveira, T. A. (2014): *BIBD, Hadamard Matrices and Combinatorial Analysis*, in Proceedings of SMTDA 2014, 3rd Stochastic Modeling Techniques and Data Analysis, International Conference in Lisbon, Portugal, 11-14 June 2014. Book of Abstracts, 61. Disponível em: http://www.smtda.net/images/Final_BOOK_OF_ABSTRACTS_SMTDA2014.pdf Acesso em 23/05/2014.

Francisco, C. & Oliveira, T. A. (2014): *Exploring links between Experimental Design and the Risk of Data Loss on QR Codes*, in Proceedings of CIAEEAR 2014, na Conferencia Internacional da Amazónia em Estatística Experimental e Análise de Risco, na Universidade Federal do Amazonas, Manaus, Amazonas, Brasil, 12-15 Agosto 2014. Disponível em: http://stat_am.cpaa.embrapa.br/. Acesso em 25/06/2014.

Francisco, C. & Oliveira, T. A. (2014): *The importance of QR Codes versus Biometric s authentication: Reviewing links to Block Designs*, 44th International Biometrical Colloquium and 4th Polish-Portuguese Workshop on Biometry , Kraków, Poland, 7-10 Setembro 2014. Disponível em: http://www.up.poznan.pl/cb44/index_en.html . Acesso em 09/08/2014.

Francisco, C. & Oliveira, T. A. (2014): *BIBD, Hadamard Matrices and new technological devices: Applications to QR Codes*, , in Proceedings of ICNAAM 2014, International Conference of Numerical Analysis and Applied Mathematics 2014 , in Rhothes, Greece, 22-28 Setembro 2014. Disponível em http://www.2014.icnaam.org/. Acesso em 15/08/2014.

Garcia, V. A. (2011): *Planeamento de Experiências: Modelos e Estruturas com Blocos*, Dissertação de Mestrado em Estatística, Matemática e Computação, área de especialização Estatística Computacional. Universidade Aberta.

Hedayat, A. & Li Shuo-Yen, R. (1979): *The trade off method in the construction of BIB Design with repeated blocks*, The Annals of Statistic, Volume 7, Issue 6, 1277-1287.

Hedayat, A. & Hwang, H. L. (1984): *BIB(8,56,21,3,6) and BIB(10,30,9,3,2) Designs with Repeated Blocks.* Journal of Combinatorial Theory, Series A 36, 73 - 91.

ISO / IEC *18004 : 2006 (E),* Secção 8.5.1, Tabela 12. Disponível em: http://www.iso.org/iso/catalogue_detail?csnumber=43655. Acesso em 21/02/2014.

Kharaghani, H. & Tayfeh-Rezaie, B. (2004): *A Hadamard matrix of order 428*. Journal of Combinatorial Designs Volume 13, Issue 6, 435–440. Disponível em: http://onlinelibrary.wiley.com/doi/10.1002/jcd.20043/abstract. Acesso em 15/04/2014.

Lint, J. H. V. & Wilson, R. M. (2002): *A Course in Combinatorics*, chapter 18.

Marshall Hall, Jr. (1986): *Combinatorial Theory*, 2nd ed. , New York, Wiley - Interscience.

Mascarenhas, V. (2008): *Planos em blocos incompletos parcialmente equilibrados*, Dissertação de Mestrado em Estatística e Optimização. Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa

Menz, Hylton B.; Latt, M. D.; Tiedemann, A.; Mun San Kwan, M. & Lord, S. R. (2004): *Reliability of the GAITRite walkway system for the quantification of temporo-spatial parameters of gait in young and older people*. Gait Posture. 20(1), 20-5.

Monteiro, A. (2013), *O Planeamento de Experiências no aperfeiçoamento de Metaheuristicas.* Dissertação de Mestrado em Estatística, Matemática e Computação, área de especialização Estatística Computacional. Universidade Aberta.

Muller, D. E. (1954): *Application of boolean algebra to switching circuit design and to error detection.* IRE Transactions on Electronic Computers, 3:6–12.

Ogata, E.; Kurosawa, K.; Stinson, D. R. & Saido, H. (2004): *New combinatorial designs and their applications to authentication codes and secret sharing schemes.* Discrete Mathematics volume 279, issues 1–3, 383–405. Disponível em http://www.sciencedirect.com/science/article/pii/S0012365X03002838. Acesso em 28/12/2014.

Oliveira, T. A. (1994): *Planos de Blocos Equilibrados Incompletos com Repetições*, Tese de Mestrado, Faculdade de Ciências da Universidade de Lisboa.

Oliveira, T. A. (1999): *Planeamento de Experiências*, Tese de Doutoramento, Faculdade de Ciências da Universidade de Lisboa.

Oliveira, T. A. ; Oliveira, A. & Correia, H. (2013): *Beyond Balanced Incomplete Block Designs: Addressing challenges, connections, applications and R* , in Proceedings of 59th ISI World Statistic Congress 2013, Hong Kong, China, 25 a 31 de Agosto.

Oliveira, T. A. & Oliveira, A. (2012): *Ineffectiveness of the FIM in selecting Optimal BIB Designs for testing block effects*, in Proceedings of COMPSTAT 2012, 701-722, Limassol, Cyprus, August, 27-31, 2012. ISBN 978-90-73592-32-2

Oliveira, T. A. & Oliveira, A. (2011): *Experimental Design: BIBD and PBIBD applications and links*. 11th annual meeting of the European Network for Business and Industrial Statistics (ENBIS-11). http://www.enbis.org/events/current/. ENBIS 2011, Universidade de Coimbra, 4 a 8 de Setembro de 2011. Disponível em: http://www.enbis.org/events/current/96_ENBIS11_Coimbra. Acesso: 23/07/2014.

Oliveira, T. A. & Oliveira, A. (2011): *Exploring the links between the BIBD and PBIBD and mathematics. Biometric Methods and Models in Current Science and Research.* Proceedings of XIXth. Summer School of Biometrics 6-10.9.2010. Faculty of Horticulture of Mendel University, Lednice, República Checa. Editors David Hampel, Jiri Hartmann and Jarolav Michálek. Published by Central Institute of Supervising and Testing in Agriculture, 1st Ed., 183-194. ISBN 978-80-7401-028-6.

Oliveira, T. A. (2010a): *Planos em Blocos Incompletos Equilibrados e Parcialmente Equilibrados (BIB e PBIB Designs): Na fronteira entre a Estatística e a Matemática*, Actas da ENSPM 2010, 8-10 Julho de 2010, Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria.

Oliveira, T. A. (2010b): *BIB Designs with Repeated Blocks: Review and perspectives.* Proceedings of ICCS-X Conference, Tenth Islamic Countries Conference on Statistical Sciences-Statistics for Development and Good Governance. Editors Zeinab Amin and Ali, S., Hadi, The American University in Cairo. ISBN 978-977-416-365-8. Volume I, 82-96.

Oyekunle, M. ; Badu-Apraku, B.; Hearne, S. & Franco, J. (2014): *Genetic diversity of tropical early-maturing maize inbreds and their performance in hybrid combinations under drought and optimum growing conditions.* Field Crops Research, Vol. 170, January 2015, 55-65. Disponível em:

http://www.sciencedirect.com/science/article/pii/S0378429014002834. Acesso em 25/06/2014.

Pearce, S. C. (1964): *Experimenting with blocks of natural size*. Biometrics 20, 699-706.

Plackett, R. L. & J. P. Burman (1946). *The design of optimum multi-factorial experiments*. Biometrika, 33, 305-325.

Preneel, B.; Dobbertin, H. & Bosselaers, A. (1997): *The Cryptographic Hash Function* RIPEMD-160, Katholieke Universiteit Leuven.

Reed, I. S. (1954): *A class of multiple-error-correcting codes and the decoding scheme.* Transactions of the IRE Professional Group on Information Theory, 4:38–49.

Reed, I. S. & Solomon, G. (1960): *Polynomial Codes over certain Finite Fields.* Disponível em: http://www.jstor.org/discover/10.2307/2098968?uid=3738880&uid=2&uid=4&sid=21104993850317. Acesso em 26/06/2014.

Richards, M.; Marder, K; Cote, L. & Mayeux, R. (1994): *Interrater Reliability of the Unified Parkinson's Disease Rating Scale Motor Examination*. Disponível em: http://www.readcube.com/articles/10.1002/mds.870090114?r3_referer=wol&tracking_action=preview_click&show_checkout=1. Acesso em 23/10/2014.

Rueda, D.; Cotta, C. & Leiva, A. J. F. (2011): *A Memetic Algorithm for Designing Balanced Incomplete Blocks.* International Journal of Combinatorial Optimization Problems and Informatics, Vol. 2, No. 1, 14-22. ISSN: 2007-1558. Disponível em: http://www.redalyc.org/pdf/2652/265219618003.pdf . Acesso em 9/08/2014.

Samad, A.; Singh, R. & Rao, S. (2012): *Bioequivalence Studies and Statistical Issues with High Variable Drugs*. Fortis Clinical Research Ltd. Sunflag Hospital & Research Centre Sector 16-A, Faridabad -121 002 (Haryana). 10-17. Disponível em: http://www.tcrp.co.in/Vol%203%20Issue%201.pdf. Acesso em 8/10/2014.

Sarkar, P. & Saha, A. (2011): *Secure Communication Using Reed-Muller Codes and Partially Balanced Design in Wireless Sensor Network*, conferência IEEE Simpósio Internacional de Processamento Paralelo e Distribuído com aplicações Workshops

SPAW. Disponível em: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5951976&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5951976. Acesso em 23/05/2014.

Sarkar, P. & Saha, A. (2011): *Security Enhanced Communication in Wireless Sensor Networks Using Reed-Muller Codes and Partially Balanced Incomplete Block Designs*, Journal of Convergence, Volume 2, Number-1.

Silva, P. (2009): *Modelos de Planos em Blocos Incompletos: revisão e perspetivas*. Dissertação apresentada na Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa para obtenção do grau de Mestre em Estatística e Optimização. Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa.

Shah, D. & Shah, Y. (2014): *QR Code and its Security Issues*, International Journal of Computer Sciences and Engineering, Vol. 2, Issue 11, E-ISSN: 2347-2693. Disponível em: http://www.ijcseonline.org/pub_paper/5-IJCSE-00589.pdf. Acesso em 15/06/2014.

Sousa, M.F. & Oliveira, T. A. (2004): *BIBDR: Some analysis on BIBD (9,24,8,3,2) cardinalities*. In Colloquium Biometryczne, Tom 34a, 2004, 161-170.

Sylvester, J. J. (1867): *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule*, ornamental tile work, and the theory of numbers, Philosophical Magazine, 34: 461-475.

Wallis, J. (1970): *Combinatorial matrices*, Ph. D. Thesis, La Trobe University.

Wang, J. & Su, R. (2008): *Further Results on the Existence of Splitting BIBDs and Application to Authentication Codes*, Acta Applicandae Mathematicae March 2010, Volume 109, Issue 3, 791-803. Disponível em http://link.springer.com/article/10.1007%2Fs10440-008-9346-8. Acesso em 28/12/2014.

Yates, F. (1936): *Incomplete randomized blocks*, Annals of Eugenics, 7, 121-140.

Yates, F. (2005): *http://www-history.mcs.st-andrews.ac.uk/Biographies/Yates.html*. Acesso em 9/3/2014.

Yue, H.; Hou, B. & Gao, S. (2014): *Note on the tight relative 2-designs on H(n,2).* Discrete Mathematics, Vol. 338, Issue 2, 6 , 196–208. Disponível em: http://www.sciencedirect.com/science/article/pii/S0012365X14003537. Acesso em 29/09/2014.

Zang, Y.; Deng, S.; Liu, Z. & Wang, Y. (2015): *Aesthetic QR Codes Based on Two-stage Image Blending*. Institute of Computer Science and Technology, Peking University, \Beijing, \P.\R. \China. \Disponível \em: http://link.springer.com/chapter/10.1007/978-3-319-14442-9_16#page-1. Acesso em 11/12/2014.

# Anexos

## Anexo I – Output do programa em BASIC utilizado para obter os PIER para k=7

```
O programa aceita K=7
Possivel existencia do PIER( 43, 86, 14, 7, 2)
Possivel existencia do PIER( 49, 112, 16, 7, 2)
Possivel existencia do PIER( 43, 129, 21, 7, 3)
Possivel existencia do PIER( 49, 168, 24, 7, 3)
Possivel existencia do PIER( 22, 44, 14, 7, 4)
Possivel existencia do PIER( 28, 72, 18, 7, 4)
Possivel existencia do PIER( 43, 172, 28, 7, 4)
Possivel existencia do PIER( 8, 8, 7, 7, 6)
Possivel existencia do PIER( 14, 26, 13, 7, 6)
Possivel existencia do PIER( 15, 30, 14, 7, 6)
Possivel existencia do PIER( 21, 60, 20, 7, 6)
Possivel existencia do PIER( 22, 66, 21, 7, 6)
Possivel existencia do PIER( 28, 108, 27, 7, 6)
Possivel existencia do PIER( 29, 116, 28, 7, 6)
Possivel existencia do PIER( 35, 170, 34, 7, 6)
Possivel existencia do PIER( 36, 180, 35, 7, 6)
Possivel existencia do PIER( 7, 7, 7, 7, 7)
Possivel existencia do PIER( 13, 26, 14, 7, 7)
Possivel existencia do PIER( 19, 57, 21, 7, 7)
Possivel existencia do PIER( 25, 100, 28, 7, 7)
Possivel existencia do PIER( 31, 155, 35, 7, 7)
Possivel existencia do PIER( 7, 8, 8, 7, 8)
Possivel existencia do PIER( 22, 88, 28, 7, 8)
Possivel existencia do PIER( 28, 144, 36, 7, 8)
```

```
Possivel existencia do PIER( 7, 9, 9, 7, 9)

Possivel existencia do PIER( 15, 45, 21, 7, 9)

Possivel existencia do PIER( 21, 90, 30, 7, 9)

Possivel existencia do PIER( 29, 174, 42, 7, 9)

Possivel existencia do PIER( 7, 10, 10, 7, 10)

Possivel existencia do PIER( 22, 110, 35, 7, 10)

Possivel existencia do PIER( 28, 180, 45, 7, 10)
```