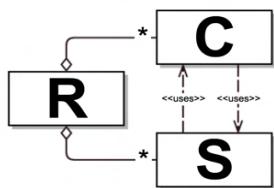




REVISTA **M**ACKENZIE DE
SISTEMAS &
COMPUTAÇÃO



UNIVERSIDADE PRESBITERIANA MACKENZIE
Faculdade de Computação e Informática



REVISTA DE COMPUTAÇÃO E SISTEMAS (RCS)

ISSN XXXX-XXXX

VOLUME 1 – NÚMERO 1 – ABRIL/2016

http://www.revistacomputacaoesistemas.net

EDITORIAL

É com grande alegria e entusiasmo que lançamos o primeiro número do primeiro volume da Revista de Computação e Sistemas (RCS).

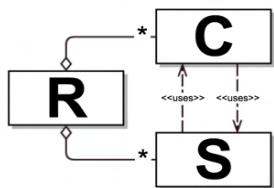
A Revista de Computação e Sistemas (RCS) é uma publicação online trimestral, cujo objetivo é divulgar pesquisas teóricas e aplicadas em Ciência da Computação e Sistemas de Informação. O acesso aos artigos da revista é público e não há taxas para processamento e/ou publicação dos artigos. O sistema de submissão de artigos é eletrônico e o processo de avaliação é realizado pelo corpo editorial e sem a identificação dos autores (*double peer reviewing in blind*).

A Revista de Computação e Sistemas publica trabalhos inéditos de pesquisa teórica e aplicada, estudos de casos e revisão bibliográfica com focos nas áreas de Ciência da Computação e Sistemas de Informação. Neste número, foram selecionados 16 (dezesseis) artigos cobrindo diversas áreas de Ciência da Computação e Sistemas de Informação: Interação Humano-Computador, Tecnologia Web, Criptografia, Realidade Aumentada, Mineração de Dados, Computação Molecular, Computação Quântica, Ambientes Virtuais de Ensino e Aprendizagem, Arquiteturas Orientadas a Serviços, Arquiteturas Corporativas e Modelos Probabilísticos em Computação.

Nossos agradecimentos a Equipe Editorial da Revista de Computação e Sistemas pelo excelente trabalho e, que este número inicial, seja uma semente muito frutífera para os próximos números desta revista.

São Paulo (SP), 11 de Abril de 2016

Prof. Dr. Israel Florentino dos Santos
Editor-Chefe da Revista de Computação e Sistemas



Unidade de Resposta Audível com Interação por Voz: Análise de Requisitos de um Estudo de Caso

Valéria Farinazzo Martins

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Rua da Consolação, 930 – CEP 01302-907 – São Paulo – SP – Brasil

valeria.farinazzo@mackenzie.br

Abstract. *Hardware and communication media evolution brought out human-computer interfaces which use a telephone keyboard or the user voice, instead of the computer keyboard and mouse. By using the voice recognition and synthesis, it is possible to achieve a more natural communication way between user and the machine. This work aims to define the main characteristics and technologies used in these types of system, including the Interactive Voice Response (IVR), which implements the interface between the user and the system available information. It also aims to show, in a case study, the user and system requirements, as well as the implementation issues.*

Resumo. *A evolução do hardware e dos meios de comunicação trouxe interfaces homem-computador que usam um teclado de telefone ou a voz do usuário, em vez do teclado e do mouse do computador. Ao utilizar o reconhecimento de voz e síntese de voz, é possível obter uma forma de comunicação mais natural entre o utilizador e a máquina. Este trabalho tem como objetivo definir as principais características e tecnologias utilizadas nestes tipos de sistema, incluindo a Unidade de Resposta Audível (URA), que implementa a interface entre o usuário e as informações disponíveis do sistema. Também se pretende mostrar, em um estudo de caso, os requisitos do usuário e do sistema, bem como as questões de implementação.*

1. Introdução

Com o desenvolvimento cada vez mais promissor dos meios de comunicação, desde a década de 90, uma nova categoria de interfaces começou a fazer parte do cotidiano, em que o usuário interage com o sistema através da fala ou de teclas de tom pelo telefone, e o sistema responde através de síntese de voz e/ou de falas pré-gravadas; estes sistemas nasceram da ideia de autoatendimento via telefone. Neste caso, o usuário, mesmo inexperiente, deve conseguir navegar pelo sistema e obter as informações necessárias. Ele deve ser capaz de interagir com um sistema que “fala”, “escuta” e “entende”.

O estado da arte em reconhecimento/síntese de voz já permite que sistemas automáticos sejam desenvolvidos para trabalhar em condições reais [San-Segundo et al 2005]. Empresas como a Nuance (2013), através do sistema Dragon (2013), a IBM

ViaVoice e a Philips Speech – compradas há alguns anos pela Nuance e a iSpeech (2013) têm investido no desenvolvimento de sistemas de voz para domínios restritos. Assim, sistemas com estas tecnologias já são comercialmente viáveis em uma grande variedade de aplicações de *Call Center*. Estas tecnologias estão, aos poucos, substituindo o menu *touch-tone* (navegação por menu) que nunca conquistou os usuários mais exigentes.

Desenvolver aplicações com reconhecimento e síntese de voz é particularmente diferente de desenvolver, por exemplo, aplicações Web. Há requisitos principalmente não funcionais que não são considerados em aplicações que utilizam mouse e teclado, tais como a naturalidade da comunicação por voz e a prestimosidade da interface. As peculiaridades dos sistemas com interface de voz fazem surgir questões ligadas a critérios de usabilidade de interface. O estudo destes critérios fez surgir o presente artigo.

O artigo está organizado da seguinte forma: no item 2 são apresentados os fundamentos conceituais Reconhecimento de Voz, Síntese de Voz, Unidade de Resposta Audível e aplicações. No item 3 é descrito o estudo de caso real. Já no item 4 são apresentados os requisitos para este tipo de aplicação. O item 5 traz alguns aspectos de implementação. Finalmente, no item 6, são apresentadas as conclusões sobre o trabalho.

2. Fundamentação Teórica

2.1. Reconhecimento de Voz

Reconhecimento de voz pode ser visto como um processo pelo qual o computador pode converter um sinal de fala acústico em um texto. A partir daí, ele é capaz de executar ações sobre a interpretação do pedido [Cohen, Giangola e Balogh 2004] [Damasceno, Pereira e Brega 2005] [Martins, Brasiliano e Fernandes 2012] [Martins et al 2013].

O processo de converter voz em texto envolve os seguintes passos [Dantas 2000], [Lamel, Minker e Paroubek 2000], [San Segundo et al 2005], [Cohen, Giangola e Balogh 2004], [Mctear 2002] [Deng e Huang, 2004] [Martins, Brasiliano e Fernandes 2012]: a) O sistema captura a palavra dita pelo usuário como um sinal acústico analógico; b) O sistema faz a conversão deste sinal analógico em componentes digitais; c) O sinal digital é fracionado em sons distintos ou segmentos; cada segmento corresponde a um som específico, tais como consoantes e vogais; d) O software de reconhecimento de voz faz a classificação do som, determinando combinações possíveis entre os segmentos de som e as representações fonéticas; e) A aplicação de reconhecimento de voz busca a palavra ou frase que mais combina com o que disse o usuário.

Este tipo de interface inclui elementos tais como: *prompts* ou mensagens do sistema, gramáticas e lógica de diálogo ou fluxo de chamada (*call flow*). Os *prompts* são todas as mensagens de voz pré-gravadas ou sintetizadas que devem ser executadas durante o diálogo com o usuário. Gramáticas definem todas as palavras, sentenças ou frases que podem ser ditas pelo usuário em resposta a um *prompt*. A lógica de diálogo define todas as ações a serem tomadas pelo sistema em determinado ponto da interação, tais como um acesso à base de dados [Cohen, Giangola e Balogh 2004]. Sobre o vocabulário utilizado, quanto maior seu tamanho, maiores serão a complexidade, as exigências e a precisão do sistema. O tamanho do vocabulário depende da aplicação a ser desenvolvida [Martins, Brasiliano e Fernandes 2012].

2.2. Síntese de Voz

Síntese de voz, do inglês Text-to-Speech (TTS), é o processo que converte texto em voz. O sintetizador recebe um texto na forma digital e o transforma em ondas sonoras, isto é, faz uma vocalização do texto. Um programa de síntese de voz é útil nas situações em que o usuário não pode desviar a atenção para ler algo ou não tem acesso ao texto escrito, seja porque a informação está distante, porque deseja realmente ouvir o texto ou porque o usuário sofre de alguma deficiência visual [Guilhoto e Rosa 2001].

Embora a tecnologia TTS ainda não reproduza com fidelidade a qualidade da voz humana gravada - vale a pena destacar que, até o momento, os sintetizadores de voz não conseguem representar entonação - ela tem melhorado muito nos últimos anos. Tipicamente, o uso da voz humana pré-gravada está atrelado aos *prompts* e ao envio de mensagens para os usuários. No entanto, determinadas aplicações, como leitores de e-mail e notícias, têm informações muito dinâmicas. Nesses casos, uma vez que os textos das mensagens não podem ser previstos, pode-se usar a tecnologia TTS para criar os discursos de saída [Cohen, Giangola e Balogh 2004].

2.3. Unidade de Resposta Audível

A utilização de URA está se tornando uma maneira popular de automação e otimização do atendimento telefônico, além de ser um canal de comunicação entre empresas. Assim como na Internet, há um esquema eficiente de relacionamento com clientes, abrindo possibilidades de diferenciação, onde a criatividade e a flexibilidade tecnológica passam a ser fundamentais para a área empresarial [Dillman et al 2009].

A URA conecta usuários utilizando um telefone com as informações que eles necessitam. Pode ser definida como um dispositivo em um sistema telefônico capaz de reproduzir as mensagens ao usuário, e também suportar as entradas deste e disparar requisições de ações para o sistema. É uma solução que permite interação com o usuário através de tecnologias como Reconhecimento de Voz Natural e de tons DTMF (Dual-Tone Multi-Frequency), Text-to-Speech e autenticação de voz [Salvador e Serrano 2003].

Os sistemas que utilizam entrada, apenas via teclado do telefone, necessitam de um menu sonoro, denominado *touch tone*; muitas vezes estes sistemas são cansativos para o usuário, pois é necessário escutar muitos menus (e em muitos níveis) para atingir a opção desejada. Embora existam técnicas, como o corte do menu, que visam melhorar a interação, estes sistemas geralmente não atingem a satisfação do usuário e começam a ser substituídos por entradas por voz. Apesar das URAs terem começado com interação por teclas do telefone, é por meio do reconhecimento de voz que se tem as maiores vantagens, pois a fala é inerente ao ser humano e sua comunicação é natural e simples. Estes sistemas, mais diretos, permitem que o usuário atinja mais rapidamente seus objetivos.

A Figura 1 mostra como é realizada a interação entre o usuário e o sistema para acesso a informações desejadas.

2.4. Aplicações Comerciais

As aplicações que utilizam URA variam bastante em grau de complexidade, visando à facilidade e agilidade de obtenção de informações tanto para o usuário quanto para o atendente humano que a ligação eventualmente possa ser direcionada. Podem ser utilizadas como parte fundamental de um sistema ou como um módulo dentro de um

sistema de telefonia mais complexo, como um sistema de celulares pré-pagos [Salvador e Serrano 2003]. São exemplos de sistemas que utilizam URA [Estabel, Moro e Santarosa, 2006] [Martins, Brasiliano e Fernandes 2012]:

- Discador Automático por Voz/Agenda - Permite que se possa realizar chamadas telefônicas a números previamente cadastrados, consultar os números telefônicos, enviar um e-mail utilizando comandos de voz, através de um telefone fixo ou celular.
- Envio de Mensagens Através do Correio Eletrônico - Através do telefone, pode-se enviar uma mensagem de correio eletrônico a um contato previamente cadastrado. É gerado um arquivo de voz que é indexado quando o e-mail é enviado.
- Notificações de Erros ou Condições Críticas no Sistema - Qualquer sistema de telefonia pode utilizar uma URA para notificar seus clientes de erros ocorridos no sistema ou condições críticas alcançadas pelos usuários, como, por exemplo, falta de créditos para executar uma chamada desde um celular pré-pago.

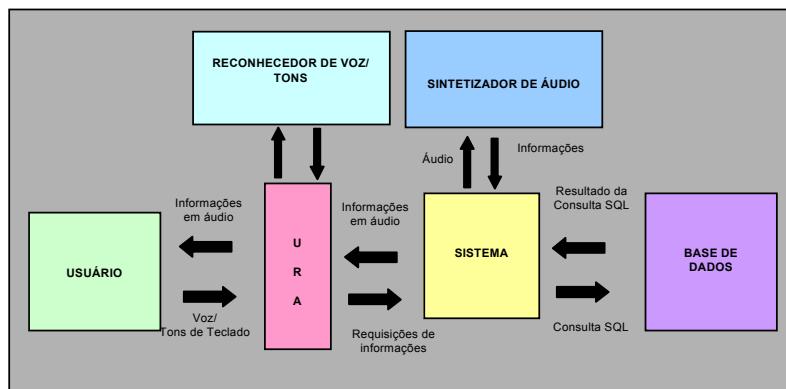


Figura 1. Arquitetura Básica de uma URA

3. Definição de um Estudo de Caso

O estudo de caso apresentado é um sistema de atendimento e transferência computadorizada de chamadas. Trata-se de um filtro que pode ser colocado quando se deseja diminuir o número de chamadas direcionadas diretamente para a telefonista. Trata-se de um caso real que foi implementado para um cliente. Os requisitos, assim como os protótipos gerados de maneira iterativa foram validados junto ao cliente e usuários reais do sistema.

O sistema deve ser capaz de reconhecer, através de voz, o nome da pessoa com quem o usuário deseja falar, ou o nome do departamento ou ainda o número do ramal. O usuário também pode, através de teclas, digitar o número do ramal, se preferir uma entrada por DTMF.

Para os casos de reconhecimento de voz, é utilizado um grau de confiabilidade para saber qual foi a taxa de reconhecimento da fala do usuário. Caso este grau de confiabilidade (configurável no sistema) seja baixo, a URA deve emitir a mensagem “Desculpe-nos, poderia repetir mais um vez?” a fim de que o sistema possa tentar reconhecer a entrada com um grau de confiabilidade maior. Se o sistema não compreender a entrada do usuário, depois de um número de tentativas de obter a

resposta, também configurável, o sistema transfere o usuário diretamente para a telefonista, tendo a URA emitido a mensagem “Desculpe-nos, estamos transferindo sua chamada para a telefonista”. Se, contudo, o grau de confiabilidade é médio, a URA deve emitir a mensagem “Você deseja falar com” composta pelo nome do usuário ou nome do departamento ou número do ramal, a fim de confirmar a entrada. Pode ainda o sistema reconhecer a entrada do usuário com grau de confiabilidade alto, em que não é necessário confirmar a entrada do usuário.

Uma vez que o sistema tenha a entrada correta do usuário, por voz ou DTMF, o sistema deve realizar uma consulta a uma base de dados que contém o ramal desejado. Outra informação vinda do resultado da consulta é se o sistema está autorizado a transferir a chamada diretamente para o ramal ou direcionar para a telefonista. No primeiro caso, a URA emite a mensagem de “Estamos transferindo sua chamada para” composta com o nome da pessoa ou do departamento ou o número do ramal. Assim, o sistema conecta o áudio do usuário com o do ramal desejado e desconecta o áudio da URA que fica liberada para um novo atendimento de chamada. Se o sistema tiver que transferir diretamente para a telefonista, a URA dará a mensagem “Estamos transferindo sua chamada para a telefonista” e o sistema conecta o áudio do usuário com a da telefonista e desconecta a URA.

4. Definição dos Usuários e Requisitos do Sistema

Requisitos são as necessidades do sistema e/ou do usuário; dizem respeito ao que o sistema deve ou não fazer e como fazer a fim de serem amigáveis para o usuário.

Um sistema deve ter seus requisitos muito bem especificados para que os erros desta fase não sejam transmitidos a fases subsequentes de projeto e implementação, desapontando os usuários, aborrecendo desenvolvedores ou mesmo podendo inviabilizar o sistema [Pressman 2004].

Seguindo uma sequência, é possível identificar os requisitos necessários desta fase:

- Definir os usuários com relação a experiências, atitudes, necessidades, capacidades humanas e motoras e desempenho;
- Qual é o ambiente em que a aplicação será usada e em qual contexto;
- Especificar os requisitos comuns a essas aplicações, os funcionais, os requisitos específicos da aplicação e os referentes à interface.

4.1. Definição dos Usuários, Tarefas e Ambientes

A definição dos usuários, tarefas e ambiente é essencial para a especificação de técnicas apropriadas de IHC que visem à criação de sistemas utilizáveis.

A eficácia da interface é um fator crucial. Questões vinculadas à utilização da representação da informação devem permitir uma nova compreensão dos dados na aplicação. Outro fator importante refere-se à usabilidade da interface. Ela deve ser avaliada de acordo com critérios como taxa de erros, tempo de execução de uma tarefa, carga de trabalho e avaliações subjetivas dos usuários. Finalmente, considerar o valor da interface no ambiente de trabalho e/ou físico em que o usuário, de fato, executa a tarefa em questão.

Os usuários. Para este tipo de sistema, não há como saber quem serão seus efetivos usuários, pois serão todas as pessoas que desejarem se comunicar com um determinado

departamento na empresa ou com alguém especificamente. É necessário que seja desenvolvido um sistema que não tenha necessidade de treinamento prévio, pois os usuários querem ser transferidos rapidamente e de maneira eficaz. Para um sistema de atendimento e transferência computadorizada de chamadas, é possível tratar usuários experientes de forma diferenciada dos principiantes. Assim, usuários experientes podem cortar a mensagem vinda da URA através de uma fala. O usuário experiente pode ainda digitar o número do ramal. Esta ação dá agilidade ao processo de transferência da chamada.

A tarefa. Na especificação dos requisitos de uma aplicação com URA, é importante que sejam definidas as metas da aplicação, as tarefas que serão necessárias para se alcançar essas metas, e como as tarefas serão realizadas no ambiente. Neste caso, o usuário pode interagir com o sistema através de voz ou de tons DTMF.

O ambiente. Em aplicações guiadas por voz, deve-se ter em mente que o usuário pode estar num ambiente físico silencioso ou com muita interferência sonora, pode estar utilizando um celular ou um telefone fixo. Assim, deve haver ajustes que controlam o volume com que a voz chega ao equipamento de reconhecimento de voz, uma tolerância a ruído e certo grau de liberdade na gramática para não tomar todas as palavras que chegam através do telefone [Salvador e Serrano 2003].

4.2. Requisitos Funcionais Comuns a Aplicações de Interface de Voz

Os requisitos comuns a aplicações de URA são os requisitos funcionais que devem ser considerados quando são projetadas praticamente todas as aplicações deste tipo, entre os quais é possível citar [Salvador e Serrano 2003]:

- Veracidade - a precisão com que a interface responde as interações do usuário, fazendo-o se sentir como se estivesse conversando com uma pessoa.
- Capacidade de Reconfiguração - é a habilidade que o sistema possui de ser modificado facilmente. Para uma URA, a facilidade de se trocar as mensagens dadas ao usuário deve ser considerada como ponto crucial, assim como configurar o grau de confiabilidade de compreensão das entradas do usuário.
- Multiusuário – deve permitir que vários usuários possam usar o sistema ao mesmo tempo. A URA deve permitir tantos usuários quanto o número de canais de entrada do PABX em que está inserida.
- Interatividade - é a capacidade do usuário poder se expressar e o sistema responder às entradas do usuário, seja através de tons DTMF ou voz.

Além disto, segundo [Mitchell 2007], [Rocha e Baranauskas 2003] e [Nielsen 2003], para se obter uma boa interface, é necessário que certos requisitos sejam atendidos:

- Diversidade – A interface deve suportar todas as classes de usuários, identificar cada usuário e adaptar-se a ele. Algumas estratégias são lançadas neste caso: desvio da chamada para atendentes ao perceber certa dificuldade do usuário; ajudas e exemplificações de uso colocadas no final de frases. Já para usuários experientes, deve haver certa diferenciação para não aborrecê-los e gerar agilidade em suas ações, como, por exemplo: ser possível cortar uma frase sem escutá-la inteira.

- Complacência – A interface deve dar suporte ao usuário, quando este fizer a recuperação de seus erros, assim como prever que o usuário se esqueça de informações já apresentadas.
- Eficiência – Deve minimizar o esforço do usuário para executar uma dada tarefa.
- Conveniência – Deve proporcionar acesso fácil a todas as operações.
- Flexibilidade – A interface deve fornecer várias maneiras para se executar uma dada operação.
- Consistência – A interface deve ter os comportamentos e a apresentação física bem definidos por regras conhecidas pelo usuário, como por exemplo: empregar sempre a mesma codificação; empregar caracteres de teclado sempre na mesma função; e mostrar as mensagens de estado do sistema em local fixo.
- Prestimosidade – A interface deve fornecer ajuda sempre que requisitada ou quando perceber que o usuário se encontra em dificuldades.
- Imitação – A interface deve explorar os aspectos de comunicação não orientados a comandos, tais como: o uso de exemplos, explanações, analogias, comparações e descrições.
- Eficiência - Se o sistema funciona adequadamente, então o esforço do usuário é mínimo visto que a interação por voz parece ser a mais natural.
- Naturalidade – A interface deve envolver o usuário de uma maneira bastante natural, não exigindo terminologia não referente à tarefa.
- Satisfação – A interface deve realizar o que o usuário espera, não o frustrando. Seu tempo de resposta deve ser suficientemente pequeno a ponto de não desmotivar o usuário e deve permitir que ele obtenha ajuda em qualquer ponto de sua interação.
- Passividade – Deve permitir que o usuário detenha o controle da interação.

Para o estudo de caso em questão, foi determinado que ele deveria atender, ao máximo, os requisitos comuns e de interface. Assim:

- Multusuário: determinado pelo número de canais do PABX disponíveis que chegam a URA.
- Capacidade de reconfiguração: é atingida através da fácil alteração de mensagens ao usuário, grau de confiabilidade de compreensão do usuário, grau de liberdade da gramática, nível de ruído permitido, etc.
- Diversidade: sistema deve guiar usuários principiantes e experientes para que ambos atinjam seus objetivos. Algumas estratégias serão explanadas na seção 5.
- Flexibilidade: Para este tipo de interface é possível realizar entrada de dados através de tons DTMF ou voz; ainda através de voz, é possível dizer o nome da pessoa, ou do departamento ou o número do ramal.
- Prestimosidade: Neste caso, se o usuário não consegue se comunicar de forma eficaz com o sistema, então este deve transferi-lo para a telefonista antes que o usuário se aborreça.

- Eficiência, Satisfação e Passividade: o sistema deve reconhecer para onde a chamada deve ser transferida rapidamente para não frustrar o usuário. Se muitas chamadas são transferidas para a telefonista porque o sistema não reconheceu a entrada do usuário, então o sistema deve ser reajustado. O sistema também deve guardar em arquivo todas as chamadas bem sucedidas e mal sucedidas a fim de que seja possível analisar o desempenho do sistema.
- Naturalidade: a própria comunicação por voz permite que a interface seja mais natural.

4.3. Algumas Recomendações sobre Interface de Voz

O projeto de interfaces de voz é bastante crítico em sistemas que trabalham como *Front end* com o usuário. Mesmo algo simples como o *touch-tone* pode ser bem ou mal projetado. Com voz, um projeto de interface deve colocar o usuário em um diálogo agradável, e não ambíguo, projetado para reconhecimento de alta precisão. Dantas (2000) descreve algumas orientações sobre a seleção de bons serviços ativados por voz:

- Um padrão de voz e um estilo próprios devem ser fixados, para permitir “personalidade” para o serviço, seja pelos apelos criados ou como são gravados.
- Múltiplas opções de navegação devem ser oferecidas. É crucial entender se tanto os usuários experientes quanto os novatos se sentirão cômodos com as instruções passo a passo e as opções de linguagem natural disponibilizadas, ou se é conveniente tratá-los diferentemente.
- Os serviços devem ser amigáveis; recomenda-se o uso de frases educadas, tais como: “sinto muito, eu não entendi” ao invés de frases técnicas como “este dado não é válido”.
- O sistema deve ser constituído de forma a induzir o usuário a solicitar naturalmente informações específicas ao invés de questões abertas. Por exemplo, deve perguntar ao usuário “Com quem você deseja falar?” ao invés de “Em que posso ajudá-lo?”.

5. Aspectos de Implementação

Os principais aspectos de implementação referentes à interface do estudo de caso são destacados a seguir.

- Controle de entradas mal sucedidas do usuário: É possível configurar a quantidade de vezes que se deseja tentar obter a correta entrada do usuário. Se, nestas tentativas, o sistema não obtiver a compreensão da fala do usuário, a chamada é transferida para a telefonista.
- Corte do menu: A fim de não frustrar e irritar usuários mais experientes que não queiram ouvir a mensagem completa vinda da URA, é possível realizar a entrada por voz; o sistema, então, corta a reprodução de áudio e tenta fazer o reconhecimento desta entrada do usuário.
- Ajuste da Porcentagem de Reconhecimento: É possível ajustar o nível em que o sistema reconheceu determinada entrada do usuário. Compreensão baixa: o sistema informa que não compreendeu corretamente a entrada e solicita que o

usuário tente novamente. Compreensão média: é feita a confirmação do usuário, repetindo a entrada que supostamente foi dada. Compreensão alta: o sistema executa a ação, podendo mencionar qual será a ação a ser executada.

- Ajuste de Interferência Sonora: Configuração do nível de ruído permitido na chamada. Isto é importante quando o usuário está num ambiente físico com barulho.

6. Conclusões

Foi verificado que sistemas que utilizam Unidade de Resposta Audível como interface devem ter seus requisitos muito bem definidos, e, além disto, devem ser levados em conta, os requisitos de interface e também as metas de interface, já que este tipo de sistema dificulta o processo de treinamento de classes de usuários. O sistema deve ser bastante natural ao usuário, como se a interação fosse entre duas pessoas.

Outro cuidado que se deve ter é o de não frustrar nenhuma classe destes potenciais usuários, proporcionando facilidades de uso àqueles usuários experientes.

O sistema deve ser bastante rápido em suas interações com o usuário, além de ser configurado de forma que se tenha um reconhecimento de voz bastante eficaz.

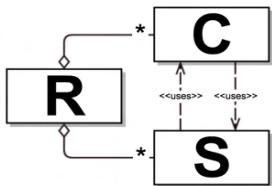
A evolução destas classes de sistemas está intrinsecamente relacionada ao estudo e ao avanço das áreas de reconhecimento de voz, autenticação e síntese de voz.

O reconhecimento de voz já começa a ser o método mais cômodo para a entrada de dados, edição de textos e computação por conversação, uma vez que a fala é o meio mais fácil e natural para diversas aplicações. Atualmente, o reconhecimento de voz permite que usuários recuperem informações de empresas e realizem transações até mais rapidamente que através da web, mediante uma linha telefônica, se o sistema for bem projetado.

Referências

- Cohen, M. H., Giangola, J. P., Balogh, J. (2004). Voice User Interface Design, Addison Wesley, ISBN 0-321-18576-5, 368 páginas.
- Damasceno, E. F.; Pereira, T. V.; Brega, J. R. F. (2005) Implementação de Serviços de Voz em Ambientes Virtuais. In INFOCOMP Journal of Computer Science, v.4, n3, p.67-73.
- Dantas, E. B. (2000). Telemarketing, A Chamada para o Futuro. Editora Atlas, 4^a edição, São Paulo.
- Dillman, D. A., Phelps, G., Tortora, R., Swift, K., Kohrell, J., Berck, J., & Messer, B. L. (2009). Response rate and measurement differences in mixed-mode surveys using mail, telephone, interactive voice response (IVR) and the Internet. Social Science Research, 38(1), 1-18.
- Estabel, L.B.; Moro, E. L.; Santarosa, L. C. (2006). A inclusão social e digital de pessoas com limitação visual e o uso das tecnologias de informação e de comunicação na produção de páginas para a Internet. Ci. Inf., vol.35, n.1.
- Ghilhoto, P. J. S., Rosa, S.P.C.S. (2001). Reconhecimento de Voz. Trabalho de Síntese para a disciplina de Sistemas Multimídia, Licenciatura em Engenharia Informática, Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

- Ispeech. Disponível em: <http://www.ispeech.org/>. Acesso em: 31/01/2013.
- Lamel, L.; Minker, W.; Paroubek, P. (2000). Towards Best Practice in the Development and Evaluation of Speech Recognition Components of a Spoken Language Dialog System, In: Natural Language Engineering, vol 6 (3-4), United Kingdom Cambridge University Press, pp. 305 - 322.
- Martins, V.F; Brasiliano, A.; Fernandes, L.F. (2012) Interface do Usuário Baseada em Voz Como Ferramenta para Promover o Ensino/Aprendizagem de Língua Estrangeira, REAVI - Revista Eletrônica do Alto Vale do Itajaí; 1^a edição, 2012, disponível em: <http://www.revistas.udesc.br/index.php/reavi/issue/view/251>
- Martins, V. F.; Santos, A. G.; Rodrigues, F. A.; Okumura, M. H.; Sakoda, T. J.; Guimarães, M. P. (2013). Análise, projeto e implementação de uma aplicação utilizando interface de voz com o usuário. In: Computer on the beach, 2013, Florianópolis. Anais do Computer on the beach 2013.
- Mctear, M. F. (2002). Spoken Dialogue Technology: Enabling the Conversational User Interface, In: ACM Computing Surveys, Vol. 34, No. 1, pp. 90–169.
- Mitchell, P.P. (2007). A step-by-step guide to usability testing, Lincoln, NE: iUniverse.
- Nielsen, J. (2003). Usability Engineering. Academic Press, Cambridge, MA.
- Nuance. Disponível em: <http://www.nuance.com/for-individuals/by-product/dragon-for-pc/index.htm>. Acesso em 31/01/2013.
- Pressman, R.S. (2004). Software Engineering. 7th ed., Addison-Wesley.
- Rocha, H. V., Baranauskas, M. C. C. (2003). Design e avaliação de interfaces humano-computador, NIED, Instituto de Computação, Unicamp, Campinas.
- Salvador, V. F. M., Serrano, D. (2003). Especificação de requisitos aplicados a sistemas que utilizam URA e um estudo de caso. In: Cadernos do Centro Universitário São Camilo, v.9, n.4, ISSN 0104-5865.
- San-Segundo, R.; Montero, J. M.; Macías-Guarasa, J.; Ferreiros, J.; Pardo, J. M. (2005). Knowledge-Combining Methodology for Dialogue Design in Spoken Language Systems, In: International Journal of Speech Technology 8, 45-66, Springer Science + Business Media.



Proposta de um módulo de avaliação de proficiência do imigrante chinês em língua portuguesa para um sistema hipermídia adaptativo

Chen P. Wang, André S. Soares, Thiago F. Penna, Maria Amelia Eliseo

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
CEP 01.302-970 – São Paulo – SP – Brasil

{wagnerchen2668, destutz}@yahoo.com.br, tpenna@click21.com.br,
mamelia@mackenzie.br

Abstract. *Adaptive Hypermedia Systems can contribute in the Portuguese language learning efficiently for Chinese immigrants. This paper shows a proposition of an evaluation module of proficiency in the Portuguese language for Chinese immigrants. This module evaluates the level of student's knowledge and proposes a plan of studies and in the future can integrate an adaptive hypermedia system from the data gotten to the evaluation module and structuring automatically the course for each student.*

Resumo. *Sistemas hipermídia adaptativos podem contribuir de forma eficiente no aprendizado da língua portuguesa por imigrantes chineses. Este artigo apresenta o processo de elaboração de um módulo de avaliação de proficiência na língua portuguesa para imigrantes chineses. Este módulo avalia o nível de conhecimento do estudante e propõe um plano de estudos, podendo, no futuro, integrar-se a um sistema hipermídia adaptativo que a partir dos dados fornecidos pela avaliação irá estruturar automaticamente o curso para cada estudante.*

1. Introdução

Muitas são as dificuldades no aprendizado de línguas estrangeiras, especialmente acentuados quando o idioma materno possui distância extrema da língua que se deseja aprender, com diferentes linguísticas, estruturas de escrita, gramática etc. Em geral os chineses chegam ao Brasil sem saber se comunicar verbalmente; o aprendizado é difícil por conta das diferenças linguísticas e culturais. As barreiras formadas por estas tornam a vida deles complexa, com dificuldade para comunicar as necessidades mais básicas como se alimentar, pedir informações, se locomover etc.

Este artigo tem como objetivo mostrar o processo de elaboração de um módulo que compõe um sistema hipermídia para avaliar a proficiência dos imigrantes chineses na língua portuguesa e indicar um programa de estudos mais adequado nesta língua, de acordo com o nível de conhecimento do aprendiz. Este módulo poderá, posteriormente, ser integrado a um sistema hipermídia adaptativo de apoio no ensino da língua

portuguesa para imigrantes chineses, que a partir dos dados fornecidos pelo módulo de avaliação irá estruturar automaticamente o curso para cada estudante.

Para alcançar estes objetivos foi necessário realizar pesquisa teórica sobre métodos no ensino da língua portuguesa para estrangeiros, como segunda língua; compreender a relação sócio-cultural dos chineses no processo de comunicação e buscar um método para a elaboração de sistemas hipermídia que auxiliem o ensino língua portuguesa para estrangeiros.

Pretende-se, assim, contribuir na minimização das barreiras impostas pela cultura e pela língua, construindo um sistema capaz de avaliar o conhecimento do imigrante chinês e indicar para ele apenas o conteúdo necessário para que se possa comunicar na língua portuguesa no menor tempo possível.

2. Sistemas Hipermídia Adaptativos

A hipermídia adaptativa trata das relações entre a organização de uma hipermídia e modelos de usuário. Os sistemas hipermídia adaptativos constroem um modelo dos objetivos, das preferências e do conhecimento de cada usuário individual, e usam este modelo durante toda a interação com o usuário, a fim de se adaptar às necessidades deste [Brusilovsky 2001].

Segundo Palazzo (2002), a “Hipermídia Adaptativa (HA) é a área da ciência da computação que se ocupa do estudo e desenvolvimento de sistemas, arquiteturas, métodos e técnicas capazes de promover a adaptação de hiperdocumentos e hipermídia em geral aos objetivos, expectativas, necessidades, preferências e desejos de seus usuários”. Possibilita a organização dos ambientes hipermídia, a condução do usuário por caminhos desejáveis, a omissão de *links* irrelevantes aos objetivos, preferências e interesses do usuário, tornando a navegação no hiperespaço mais atrativa e organizada, de acordo com o perfil e as necessidades que estão representados no Modelo do Usuário [Palazzo 2002].

Segundo Oliveira e Fernandes (2004), o Modelo do Usuário representa as preferências, conhecimentos, objetivos, histórico de navegação e outros aspectos relevantes. O modelo de referência exposto por Oliveira e Fernandes (2004), exemplifica um modelo de curso adaptativo completo, conforme Figura 1. A Interface é a apresentação do sistema onde ocorre a interação com o usuário. O Analisador da interação se encarrega de selecionar e guardar informações relevantes sobre o usuário e sobre sua interação com o sistema. O Modelo do Aprendiz contém as características do aprendiz, e o que o sistema “sabe” sobre ele, traçando um perfil do usuário. O Modelo de decisão de adaptação tem a função de decidir quando e o que deverá ser adaptado. O Gerador de apresentação é a etapa final do processo de adaptação, ele reúne informações dos módulos anteriores para apresentar os resultados ao usuário. O Modelo da aplicação é um módulo composto por três partes com funções bem definidas, a saber:

- Submodelo de domínio: armazena informações sobre como os dados estão estruturados na aplicação;
- Submodelo de Hiperbase: responsável pelos materiais relativos ao curso a ser aplicado, como exercícios, exemplos, avaliações e outros conteúdos, incluindo os dados descritos no modelo instrucional;

- Submodelo Instrucional: informa a aplicação qual é o projeto principal do curso, qual é o modelo padrão a ser seguido.

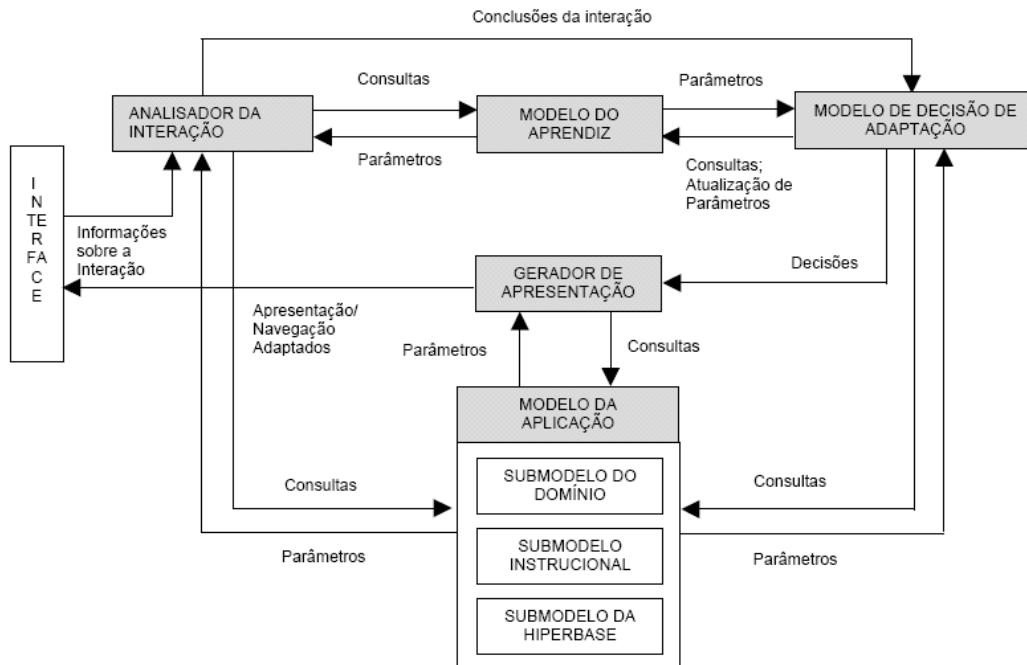


Figura 1. Modelo de curso adaptativo. Fonte: OLIVEIRA e FERNANDES (2004)

O módulo de avaliação em proficiência na língua portuguesa proposto utiliza como subsídio o “Modelo do aprendiz” de um sistema hipermédia adaptativo, ao retornar os resultados dos testes feitos pelos usuários. É importante ressaltar que o objetivo deste módulo, além de avaliar o imigrante, é prover como resultado desta avaliação um diagnóstico que possa ser utilizado como base no “Modelo de Aprendiz” apresentado por Oliveira e Fernandes (2004).

3. As necessidades do imigrante Chinês no aprendizado da língua portuguesa e os requisitos do sistema

Este capítulo mostra as necessidades do imigrante chinês como aprendiz de língua portuguesa com o objetivo de estabelecer os requisitos que o módulo de avaliação deverá contemplar.

Para o levantamento das necessidades do público alvo foi feita uma pesquisa de campo com 46 imigrantes Chineses alfabetizados na língua mãe, envolvendo tanto crianças quanto adultos. Nesta pesquisa, cada participante respondeu a um questionário com perguntas sobre a impressão que o imigrante tem sobre si, sobre o seu aprendizado e dificuldades na língua portuguesa e ao final foi solicitado que cada entrevistado fizesse uma redação.

A partir da análise dos questionários, foi possível perceber que o conteúdo das redações trazia os motivos que trouxeram o imigrante a morar no Brasil, falava sobre

suas dificuldades e suas impressões a respeito da cultura. A análise ortográfica mostrou a existência de padrões de erros em gramática e concordância.

Para realizar a análise quantitativa as redações foram inseridas em uma matriz contendo dados como quantidade de palavras, quantidade de erros no geral e quantidade de erros subdivididos em alguns ramos principais da língua portuguesa, citados mais abaixo. Foram considerados apenas 38 questionários, pois dentre os 46 pesquisados, 8 não se dispuseram a redigir a redação. Durante a análise as palavras de todas as redações foram contadas e somadas, totalizando 2383 palavras, deste total 273 foram escritas de forma errada ou em um contexto incorreto na frase, o que nos dá 11,46% de erros identificados.

Estes erros foram contabilizados em cada ramo da língua portuguesa: gramática, concordância, vocabulário, pronome, adjetivo, uso de gênero, uso de plural, artigo e verbos, conforme a Figura 2.

Da análise quantitativa podem ser retirados alguns dados sobre o perfil dos pesquisados:

- A maior dificuldade na comunicação destes imigrantes está no uso de verbos, artigos e plural;
- A idade parece interferir no aprendizado, tanto positiva como negativamente, ou seja, pessoas mais velhas têm maior dificuldade no aprendizado e crianças têm grande facilidade;
- A pesquisa objetiva não está batendo com a análise das redações em 66% dos casos, o que indica que 66% dos imigrantes pesquisados não sabem aos certo o que mais o prejudica na sua comunicação na língua portuguesa.

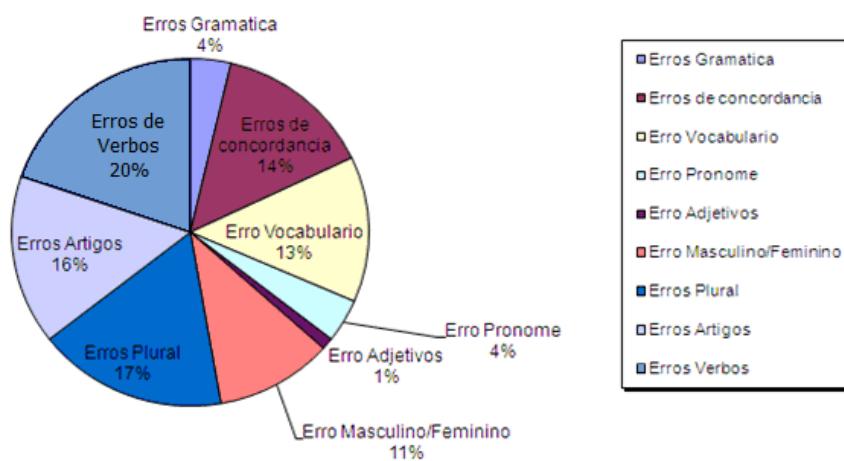


Figura 2. Percentuais de erros dos imigrantes

A análise qualitativa foi feita a partir da leitura de cada redação, identificando pontos de interesse do imigrante sobre a cultura brasileira, suas dificuldades ao chegar ao Brasil, pontos importantes da sua cultura e demais dados relacionados. Todos os pesquisados vieram com toda a família e não sabiam praticamente nada sobre o Brasil ao se mudarem. Destacam as diferenças culturais e demonstram curiosidade sobre a

cultura brasileira, língua portuguesa e os costumes. Os imigrantes revelaram não dispor de muito tempo, esta condição deve ser observada quando da montagem do sistema, pois os testes devem durar o mínimo possível. Os imigrantes destacam também sua dificuldade no aprendizado da língua portuguesa. Para entender melhor as dificuldades do imigrante chinês a Tabela 1 faz um comparativo entre estruturas gramaticais existentes no português e no chinês, mostrando as diferenças entre as duas línguas.

Tabela 1: Comparação entre a estrutura gramatical da língua portuguesa e a língua chinesa. Fonte: Weiki, 2008.

Comparação entre as línguas portuguesa e Chinesa	
Português	Chinês
Artigo - o, a (Masculino Feminino).	Não existe
Pronomes Possessivos - meu, minha, seu, sua, nosso, nossa (Masculino Feminino).	1 ^a e 2 ^a pessoas do singular e plural não diferenciam masculino e feminino 3 ^a pessoa do singular e plural diferencia masculino e feminino
Pronome Demonstrativo - este, esta, esse, essa, aquele, aquela (Masculino Feminino).	Não existe
Adjetivo - bonito, bonita, magro, magra, bom, boa, mau, má, cru, crua (Masculino Feminino).	Não existe
Verbo Regular e Irregular - presente, pretérito perfeito, pretérito imperfeito, futuro.	Não existe
Substantivo Plural - casas, mesas, livros, jornais, sinais, fáceis, répteis, papéis, hotéis, pastéis, moveis, luzes, gases, álbuns, irmãos.	Não existe
Ordem de frases - substantivo sempre esta a frente do adjetivo - Ex: O carro bonito	Ordem de frase- o adjetivo sempre vem antes do substantivo - Ex: O bonito carro

3.1. Metodologias de ensino de língua portuguesa como segunda língua

Existem em uso alguns métodos de ensino de português para estrangeiros, compreendendo sequências de aprendizado específicas e eficientes, cada vez mais sendo aperfeiçoados, dando lugar a métodos mais modernos.

O método para avaliação de proficiência na língua portuguesa utilizado no levantamento de requisitos para o módulo de avaliação na proficiência da língua portuguesa proposto foi o “*Interchange for International Communication*” usado no ensino da língua inglesa [Reis 1998]. A escolha deste método está baseada nos princípios colocados por Reis (1998): “o objetivo é apresentar a língua como ela é utilizada em suas funções comunicativas, pois é por meio de sua utilização que ela dá forma ao sistema”. Usou-se como apoio, para a implementação deste módulo, o curso contido no livro “*Muito prazer*” que epistemologicamente, muda o código de ensino de inglês, como segunda língua, para português, baseando-se no método “*Interchange for International Communication*” [Fernandes, Ferreira e Ramos 2008]. Dentre os métodos de ensino de segunda língua pesquisado, este foi o que se mostrou mais adequado para o ensino da língua portuguesa para chineses.

3.2. Requisitos do sistema

A partir da pesquisa de campo e do levantamento bibliográfico sobre os métodos de ensino de língua estrangeira, conclui-se que o módulo de avaliação de proficiência na língua portuguesa deve contemplar os seguintes requisitos:

- O sistema deve apresentar um conteúdo voltado para a cultura brasileira;
- O imigrante chega ao Brasil sem entender a língua portuguesa, por isso o sistema deve explorar imagens, animações e/ou vídeos, sendo mais visual possível;
- O sistema deve ser voltado para um curso dirigido, pois 66% dos pesquisados não conseguem identificar suas reais necessidades na comunicação em português;
- O sistema deve preferencialmente ter módulos de aprendizado separados para adultos e crianças, pois as crianças aprendem mais rapidamente;
- A maior dificuldade do imigrante está em aprender a conjugação de verbos, plural e artigos e o sistema deve avaliar estas partes em especial;
- Na pesquisa de campo os imigrantes revelaram não dispor de muito tempo para entrevistas ou testes, por isso avaliação deve durar o mínimo possível;
- Revelou-se que a parte pedagógica, ou método, utilizado no sistema é de vital importância para que o resultado seja satisfatório, por isso o sistema deve utilizar o método escolhido e realizar as avaliações através dele.

3.3. Seleção e normalização do conteúdo do “Muito Prazer”

Como base para a implementação do módulo foi utilizado o método de ensino de português como segundo idioma apresentado no livro “Muito Prazer”, de Fernandes, Ferreira e Ramos (2008). As questões utilizadas para compor a avaliação de proficiência na língua portuguesa do módulo proposto foram retiradas deste livro, que está dividido em 20 unidades subdivididas em três competências:

- Verbo: quase todas as unidades mencionam este assunto, apenas variando na dificuldade.
- Gramática: as unidades do método disponibilizam este material também de forma gradativa, em ordem de dificuldade.
- Vocabulário: no método cada unidade tem um tema principal que faz com que os vocabulários relativos a determinados ambientes sirvam de pano de fundo para a inserção de formas gramaticais e verbos.

Para o módulo proposto foram elaboradas oito questões de cada unidade, o que gera um total de 160 questões para a avaliação do imigrante chinês. Cada uma das perguntas foi formulada utilizando os conceitos descritos em cada unidade, mesclando gramática, verbo e vocabulário. A partir dos resultados obtidos na avaliação, um sistema hipermídia adaptativo que utilize este módulo como avaliação e identificação do perfil do estudante poderá adaptar o conteúdo do curso conforme a necessidade do imigrante.

4. O módulo de avaliação em proficiência na língua portuguesa

O módulo de avaliação em proficiência na língua portuguesa proposto consiste em um questionário com 20 níveis de perguntas, cuja dificuldade aumenta gradualmente. Cada nível contempla um capítulo do livro “Muito Prazer”, de Fernandes, Ferreira e Ramos (2008). O sistema é composto pelos seguintes elementos:

- Um imigrante, ou seja, usuário conectado ao sistema;
- Tela de cadastro de usuários;
- Tela de avaliação, que apresenta as questões para a realização da avaliação de proficiência na língua portuguesa;
- Tela de resultados, que apresenta os resultados da avaliação para o usuário.

Para iniciar a avaliação o imigrante deve entrar no sistema e fazer um prévio cadastro com seus dados pessoais. Após efetivar o cadastro, o imigrante é direcionado para a tela de avaliação onde serão aplicados os testes, que consistem em questões de múltipla escolha. O imigrante deve sempre escolher uma das opções disponíveis e clicar em prosseguir. Cada nível é composto de oito questões, e a cada questão respondida o sistema mostra a próxima questão e atualiza os dados informando o progresso do imigrante durante a avaliação.

Se conexão de internet for interrompida durante a avaliação ou se o imigrante desejar interromper o teste basta fechar o navegador, e quando retornar deverá informar ao sistema seu *Login* e Senha cadastrados anteriormente. Ao realizar esta ação o sistema retorna os testes do ponto onde o usuário parou.

Ao término dos 20 níveis de questões o imigrante é automaticamente direcionado para a tela de resultados, onde é mostrado o resultado dos seus testes e a indicação de quais competências precisam ser aperfeiçoadas e em que ordem elas deverão aparecer para o sucesso do aprendizado na língua portuguesa.

4.1. Montagem do modelo de Banco de dados

Para o módulo de avaliação em proficiência na língua portuguesa foi elaborado um banco de dados em MySQL Server 4.1 devido a sua estrutura segura e de baixo custo. O banco de dados armazena:

- Dados cadastrais dos imigrantes (Nome, Idade, Sexo, Email);
- Dados de objetos de avaliação (os 20 níveis de aprendizado);
- Testes de cada unidade de avaliação (as questões de avaliação pertencentes a cada unidade);
- Histórico de cada usuário (perfil de cada usuário após utilizarem o sistema).

4.2. Desenvolvimento dos casos de uso do sistema

De acordo com Furlan (1998), a UML (*Unified Modeling Language*) pode ser usada para mostrar as fronteiras de um sistema e suas funções principais utilizando atores e casos de uso.

A Tabela 2 mostra os casos de uso cadastrar imigrante, realizar login e preencher avaliação pertencentes ao módulo de avaliação em proficiência na língua portuguesa. A tabela 2 também apresenta os atores e os objetivos de cada caso de uso.

Para facilitar o acesso ao módulo de avaliação de proficiência em língua portuguesa, optou-se por uma plataforma web. O módulo foi desenvolvido em ASP.NET devido a fácil integração com o MySQL.

Tabela 2: Tabela de casos de uso do módulo de avaliação em proficiência na língua portuguesa

EVENTO	ATOR	OBJETIVO
1 - Cadastrar Imigrante	Imigrante	<ol style="list-style-type: none">1. Imigrante entra no sistema.2. Sistema apresenta tela inicial.3. Imigrante clica em "Cadastrar Novo usuário".4. Sistema apresenta a tela de cadastro a ser preenchida seus dados.5. Imigrante preenche o cadastro e clica em "Cadastrar".
2 – Realizar Login	Imigrante	<ol style="list-style-type: none">1. Imigrante entra no sistema.2. Sistema apresenta tela inicial.3. Imigrante preenche seu Login e Senha.4. Imigrante clica em "Entrar".
3 - Preencher avaliação	Imigrante	<ol style="list-style-type: none">1. Imigrante escolhe uma das opções apresentadas na tela.2. Imigrante responde ao teste e clica na seta à direita para prosseguir.3. Sistema atualiza “Modelo de aprendiz” com informação do teste realizado.4. Imigrante continua respondendo as questões até o final.5. Sistema exibe o resultado dos testes na tela para que o imigrante saiba onde tem mais dificuldades.

4.3. A Interface

Para atender os requisitos expostos anteriormente, a interface foi projetada de forma a privilegiar a utilização de ícones para facilitar o entendimento. As frases utilizadas nos testes são curtas e objetivas. O menu do lado esquerdo mostra em qual unidade o imigrante se encontra e qual é a sua nota nos testes já realizados, conforme Figura 3. Na parte inferior central da tela o imigrante tem uma visão do todo, pois é informado o quanto ele já avançou nos exercícios. Na parte central onde aparecem os exercícios, existe apenas um botão, onde ele pode prosseguir.

A cada questão respondida o sistema mostra, automaticamente, a próxima questão e atualiza os dados que informam o progresso do imigrante na avaliação, que são:

- Menu a esquerda é atualizado com o progresso do imigrante no nível atual e também com a nota do imigrante na avaliação do nível atual;

- Contador na parte inferior é atualizado mostrando a porcentagem da avaliação já concluída pelo imigrante.

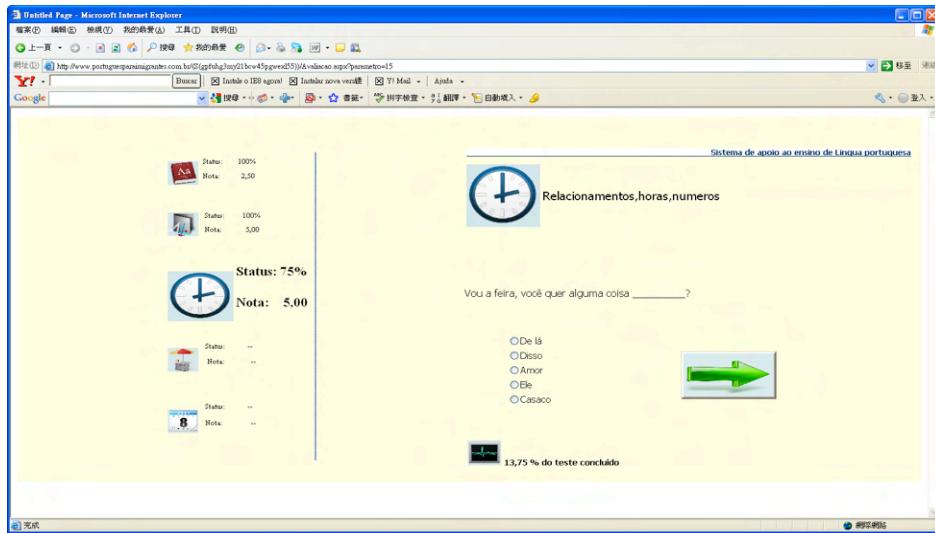


Figura 3. Tela de avaliação

4.4. Validação do sistema

Concluída a implementação do módulo de avaliação em proficiência na língua portuguesa, o sistema foi aplicado a oito imigrantes chineses, com média de idade de 30 anos, a maioria com nível superior ou nível médio de aprendizado na língua mãe, que preencheram a avaliação. Não apresentaram problemas com o funcionamento do sistema, nem dificuldades em como operá-lo. A única observação que três deles fizeram é que o teste é bastante repetitivo e um pouco extenso.

A validação feita pelos imigrantes mostrou que os requisitos apontados no item 3.2 foram atendidos satisfatoriamente:

- O sistema possui conteúdo voltado para a cultura brasileira, por isso foi utilizado o método “Muito prazer”, que mostra em suas lições a cultura e os costumes brasileiros;
- Foram utilizados ícones e componentes visuais e o mínimo de textos, para que o imigrante não se sinta confuso com a interface, tornando o sistema o mais visual possível e com uma navegação seja simples;
- A avaliação foi projetada de forma linear, para que o imigrante seja avaliado em seu conhecimento de forma gradativa, voltado para um curso dirigido;
- No que diz respeito ao fato de ter módulos de aprendizado separados para adultos e crianças, o sistema identifica da idade do imigrante através da informação cadastral preenchida inicialmente, fornecendo esta informação para que o sistema hipermídia adaptativo possa se adaptar conforme o perfil do usuário;
- Quanto ao aprendizado da conjugação de verbos, que não existe no idioma chinês, o método “Muito prazer” reforça o ensino de formas verbais, incluindo conjugações e tempos;

- As questões de avaliação foram projetadas para que o imigrante não perca muito tempo durante sua realização; o mesmo pode interromper o processo a qualquer momento e retornar, posteriormente de onde parou, sendo que esta funcionalidade mostrou-se satisfatória nos testes de validação;
- Quanto à parte pedagógica, adotou-se o método “Muito Prazer”, que se mostrou eficiente durante a validação.

5. Considerações finais e trabalhos futuros

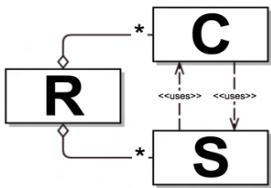
Este artigo apresentou o processo de pesquisa e implementação de um módulo de avaliação em proficiência na língua portuguesa para imigrantes chineses que poderá ser integrado a um sistema hipermédia adaptativo ao fornecer dados relativos ao nível de conhecimento, traçando o perfil do estudante. O módulo, no final da avaliação apresenta um plano de estudos adequado à necessidade do usuário.

O sistema hipermédia adaptativo pode otimizar o tempo de aprendizado do imigrante, que muitas vezes tem pressa para se comunicar na língua portuguesa. A partir dos testes do módulo de avaliação o sistema poderá indicar um conteúdo específico para cada estudante, evitando assim que ele perca tempo estudando pontos da língua portuguesa que já tenha proficiência.

Como trabalhos futuros são sugeridos a implementação de um sistema hipermédia adaptativo de ensino da língua portuguesa que utilize o módulo de avaliação apresentado neste artigo, um estudo da viabilidade de incluir interfaces orientadas a comunicação, que capturem e interpretem a fala dos usuários em linguagem natural, para ensino de línguas. E finalmente propõem-se uma avaliação de usabilidade das interfaces do módulo, a fim de verificar sua eficiência e eficácia na comunicação.

Referências

- Brusilovsky,P. (2001) *Adaptive Hypermedia. User Modeling and User-Adapted Interaction*.
- Fernandes, G., Ferreira, T. L. S. B., Ramos, V. L. (2008) *Muito Prazer, fale o português do Brasil*, Disal.
- FURLAN, José Davi. (1998) *Modelagem de objetos através da UML – The Unified Modeling Language*, Makron Books.
- Oliveira, J. M. P, e Fernandes, C. T. (2004) “Educational Adaptive Hypermedia Systems: Brief Overview and Reference Model,” In: CONAHPA Congresso Nacional de Ambientes Hipermedia para Aprendizagem. UFSC.
- Palazzo, L. A. M. (2002) “Sistemas de Hipermédia Adaptativa”, In Anais do XXII Congresso da Sociedade Brasileira de Computação (SBC), Florianópolis.
- Reis, Mariza. (1998) *A importância da competência gramatical no ensino comunicativo (em língua inglesa)*, Oficina de Textos.
- Weiki, Zhang. (2008) *Diferenças culturais e tradução*. Universidade de estudos internacionais de Xangai.



Anotações Semânticas para Query-by-Humming

Danieli P. de Sousa, Luciano Silva

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
São Paulo – SP – Brasil
danip.sousa@gmail.com, luciano.silva@mackenzie.br

Abstract. *A difficulty reported by many people is to find the name or the artist of a song when there is no mention or reminder of its textual elements; or when these data are uncertain and do not match with the music which information are been searched. The method of Query-by-humming has been studied for this recovery purpose. This research aims to use the CALIPH (software for semantic annotation) and EMIR (a software for data recovery which are semantically referenced by use of the CALIPH) for storage and retrieval, respectively, of images that refer to the data obtained by humming.*

Resumo. *Uma dificuldade relatada por muitas pessoas é a de pesquisar o nome ou intérprete de uma música quando não há nenhuma referência ou lembrança de elementos textuais desta; ou quando estes dados são incertos e não correspondem à música sobre a qual se busca informações. O método de query-by-humming tem sido estudado com este propósito de recuperação. A presente pesquisa tem como objetivo a utilização do CALIPH (software para anotação semântica) e do EMIR (um software para recuperação de dados semanticamente referenciados pelo uso do CALIPH) para o armazenamento e a recuperação, respectivamente, de imagens que referenciem dados obtidos by humming.*

1. Introdução

Muitas vezes ouve-se uma música, mas não se sabe o nome ou o intérprete da mesma. Por essa razão, a implementação de mecanismos de consulta a bases de dados musicais que possibilitem ao usuário encontrar informações sobre determinado arquivo de áudio apenas fundamentando em um trecho ouvido do mesmo que se guardou na memória tornou-se algo tão relevante diante desse problema tanto de usuários leigos como de profissionais ligados à música (Lau *et al.*, 2007).

Uma das técnicas que pode ser exploradas para a consulta em banco de dados de áudio que atenda a este requisito é a de *Query-by-Humming* (*QBH*). Entretanto, por lidar com linguagem natural, esta técnica encontra dificuldades de implementação, devido a discrepâncias entre o resultado que deveria ser retornado em uma consulta e o resultado que muitas vezes é efetivamente obtido. Novas propostas de implementação de armazenamento e recuperação em sistemas *QBH* são objetivos de pesquisas dentro

da área da Computação denominada Computação Musical.

Com motivação neste cenário, propõe-se analisar a viabilidade do uso da representação semântica como aliada à implementação de *QBH*. Para tanto, serão utilizados dois softwares fundamentados no padrão *MPEG-7*, o *CALIPH* e o *EMIR*. Mais concretamente, a proposta do trabalho é que voluntários simulem trechos de músicas previamente selecionadas e que estas simulações sejam armazenadas no *CALIPH* (o qual pode ser compreendido como construtor de uma base de dados anotados semanticamente) e o *EMIR* (especialmente desenvolvido para uso conjunto com o primeiro), o qual se comporta como a interface de busca do *CALIPH*.

2. Banco de Dados Multimídia para Áudio

2.1. Conceito e Estrutura de um Banco de Dados Multimídia

Segundo Elmasri e Navathe (2007), um Banco de Dados Multimídia é uma estrutura que armazena, gerencia e possibilita a recuperação de dados multimídia (desde textos, gráficos, arquivos de áudio, imagens, ou vídeos, ou ainda a combinação de todos estes dados) no formato digital. O modo como o qual um dado multimídia é armazenado varia de acordo com a classificação do mesmo. Isto significa dizer que, para cada tipo de conteúdo multimídia que se pretende armazenar, deve-se selecionar uma técnica de representação adequada. Tão importante quanto definir a forma de representação de um dado multimídia em um banco de dados multimídia é definir os tipos de consulta que serão realizadas neste banco. Considerando-se a quantidade de dados que uma aplicação multimídia, geralmente, tem de manipular, chega-se à conclusão de que as estruturas de armazenamento destes dados são complexas, o que inclusive é um dos grandes problemas na questão do armazenamento de dados multimídia.

Diante desta problemática, o uso padrões de auxílio à descrição e compressão de dados multimídia, como o MP3 (*MPEG 1 Layer-3*) para áudio, JPEG (*Joint Photographic Experts Group*) para imagens e o MPEG (*Moving Picture Experts Group*) para áudio e vídeo tem sido fundamentais para a tentativa de lidar com este problema. A seguir, será tratada a maneira pela qual um conteúdo de áudio pode ser representado em um banco de dados multimídia.

2.2. Representações de Arquivos de Áudio em um Banco de Dados Multimídia

De acordo com Kosh e Döller (2005), a tarefa de representar dados multimídia pode ser subdividida em dois tipos: a representação de alto nível e a representação de baixo nível. A representação de baixo nível compreende a maneira como o dado multimídia será reconhecido e inserido no banco. Em soluções de mercado como o *Oracle 10g* e *IBM DB2*, objetos como áudio são definidos como um tipo de dados específico, denominado *BLOB* (*Binary Large Objects*). Desse modo, a manipulação de conteúdos multimídia era generalizada, sendo o *BLOB*, portanto, um objeto de representação geral, que utiliza um vetor de *bytes* para o armazenamento dos dados multimídia no banco. Entretanto, esta representação de baixo nível não disponibiliza mecanismos necessários para a realização da consulta e recuperação dos dados de modo eficiente (ou seja, o retorno bem sucedido da busca), bem como a maneira como a consulta será realizada para que este requisito tenha sido atendido. Neste cenário, faz-se necessária uma representação

de alto nível do áudio, para que esta realize uma intermediação entre o objeto *BLOB* e a aplicação que utilizará o banco de dados multimídia.

Esta representação denomina-se representação semântica. Ela permite um tratamento diferenciado dos arquivos de áudio (e de outros tipos de conteúdo multimídia), por tornar a própria representação do conteúdo uma ferramenta de auxílio à sua consulta, porém utilizando características encontradas por meio da análise do mesmo. Ferramentas têm sido criadas com o objetivo de tornar essa representação eficiente a ponto de otimizar os resultados de consulta. A seguir, serão introduzidos dois importantes padrões de descrição de conteúdo multimídia para a realização de anotação semântica em dados: o *MPEG-7* e o *MPEG-21*.

2.3. Padrões de Descrição de Conteúdo Multimídia MPEG-7 E MPEG-21

Os padrões *MPEG-7* e *MPEG-21* foram desenvolvidos por um grupo de pesquisa ligado à *ISO (International Standard Organization)*, denominado *Moving Pictures Experts Group (MPEG)*. O padrão *MPEG-7* é também denominado Interface de Descrição de Conteúdo Multimídia. A realização de uma descrição em *MPEG-7* depende de um conjunto de metadados, somados à estrutura e conexões existentes entre os mesmos. Este padrão é totalmente centralizado na descrição do conteúdo, sendo as definições no que se referem aos mecanismos de busca a serem utilizados com o auxílio deste ou os modos pelos quais este pode ser aplicado a um sistema multimídia, tarefas não definidas em seu escopo. Este padrão é constituído por três elementos principais: Descritores (D), Esquemas de Descrição (ED) e Linguagem de Definição de Descrição (LDD), além da definição de uma outra representação, a representação binária (BiM), conforme mostrado na Figura 1, a seguir:

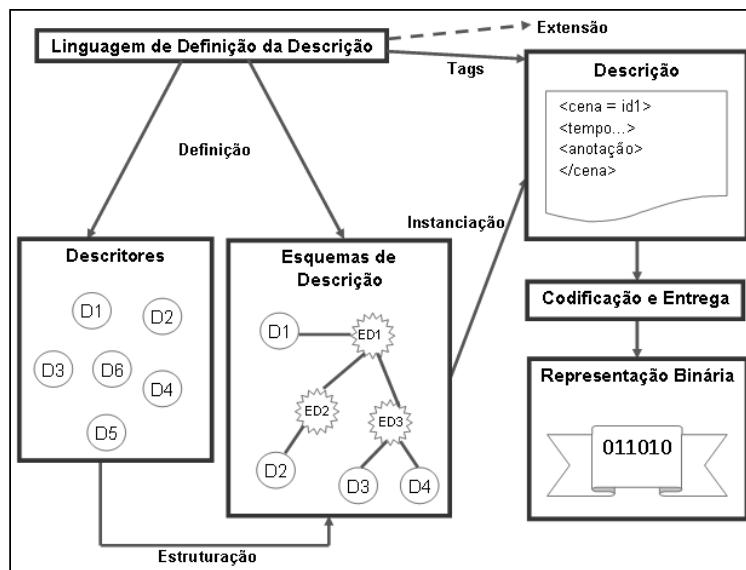


Figure 1. Principais elementos do padrão MPEG-7 [adaptada, Sonera (2003)]

A descrição em MPEG-7, em uma de suas formas de representação, utiliza-se da chamada Linguagem de Definição da Descrição (LDD), ou Linguagem de Definição da Descrição. Uma LDD emprega a sintaxe da *XML* (*eXtensible Markup Language*) para originar novos descritores e esquemas de descrição. A *XML* proporciona o uso de marcadores definíveis, as quais tornam esse tipo de linguagem favorável à criação de esquemas de descrição. É importante ressaltar que a validação de um documento de descrição nesta linguagem é realizada com fundamentação em uma gramática denominada DTD (*Document Type Definition*), conforme mencionado em Sonera (2003). O padrão *MPEG-7*, juntamente com os padrões *MPEG-1*, *MPEG-2*, *MPEG-4*, foi a base para o desenvolvimento do padrão *MPEG-21*. O padrão *MPEG-21* surgiu da necessidade de uma normalização mais abrangente no sentido de construção de um verdadeiro *framework* multimídia que pudesse facilitar a manipulação da crescente quantidade de dados multimídia inseridos em grande parte das aplicações distribuídas (sobretudo as aplicações para a Internet).

Sua composição engloba sete seguintes áreas fundamentais:

- Declaração do Item Digital;
- Descrição e Identificação do Item Digital;
- Uso e Manuseio de Conteúdo;
- Proteção e Gerenciamento da Propriedade Intelectual;
- Redes e Terminais;
- Representação de Conteúdo e Relatório de Eventos.

Para representá-lo, é utilizada o que se denomina Linguagem de Declaração de Item Digital (LDID), a qual por sua vez é definida em esquemas *XML* (assim como a Linguagem de Definição da Descrição, LDD, do padrão *MPEG-7*). A Declaração do Item Digital (DID) consiste justamente no documento *XML* que se refere a um Item Digital, de acordo com os padrões acordados na LDID. Pode-se perceber que a maneira como o *MPEG-21* realiza a representação dos dados multimídia é similar a que ocorre no *MPEG-7*.

3. *Query-by-humming*

Query-by-humming (*QBH*), de acordo com Tripathy *et al.* (2009), é um termo que pode ser compreendido como “conceito de interação na qual a identificação de uma canção tem de ser revelada rapidamente e ordenadamente, a partir de uma dada entrada de áudio cantada, utilizando um grande banco de dados de melodias conhecidas”. Uma aplicação multimídia *QBH*, portanto, caracteriza-se por possibilitar ao usuário buscar informações como nome, gênero, autores e intérpretes, além do próprio arquivo de áudio correspondente a uma música, sem que este saiba palavras que existam na composição da mesma. Como não há uma tradução técnica oficial para o referido termo, em Português pode-se compreendê-lo como “consulta pelo assovio ou solfejar”. Além de identificar os componentes de um sistema *QBH*, é necessário compreender como estes interagem para alcançar a finalidade proposta por uma aplicação deste tipo. O

componente **Entrada de Áudio** pode ser também denominado áudio *humming*, considerando que este é o arquivo que contém a gravação da melodia produzida pelo usuário do sistema na realização da consulta. As **Entradas do Banco de Dados Multimídia** são as canções previamente armazenadas no banco de dados multimídia do sistema.

Como mencionado em Unal *et al.* (2008), para que ambas as entradas sejam eficientemente comparadas, estas deverão ser convertidas em um formato similar, o qual é a **Representação Melódica**. Com fundamento nesta representação, o mecanismo de **Comparação** busca as similaridades entre os arquivos, e ao encontrar, dentre os armazenados no banco de dados, o que mais apresente similaridades com o áudio *humming* pelo usuário e realiza a recuperação do arquivo em seu formato original, juntamente com as respectivas informações associadas ao mesmo. Entretanto, um dos fatores limitantes a resultados totalmente corretos nesta busca são as imperfeições e variações presentes no áudio *hummed*.

4. Proposta

Serão apresentadas as ferramentas *CALIPH* e *EMIR*, ambas voltadas para uso com imagens e fortemente relacionadas ao padrão *MPEG-7*.

Como descrito em Lux (2009), o *CALIPH* (“*Common and Light Weight Photo Annotation*”) é uma ferramenta fundamentada na linguagem Java, cujo objetivo é realizar, sobretudo em arquivos de imagens, a tarefa de anotação semântica e de extração de metadados contidos nestes. Para a manipulação dos metadados, o *CALIPH* utiliza-se do padrão *MPEG-7*. Esta ferramenta livre possibilita a realização manual ou automática da anotação semântica. Neste trabalho, será priorizada a realização de anotação manual, a qual inclusive pode ser realizada de diferentes formas, de acordo com o objetivo específico que se pretende alcançar ou pela forma como será realizada a busca do arquivo em que foi efetuada a anotação.

EMIR (Experimental Metadata based Image Retrieval), de acordo com Lux (2009), é uma ferramenta desenvolvida em Java para ser utilizada em conjunto com o software *CALIPH*, possibilitando a realização de buscas em arquivos anotados semanticamente pelo mesmo, conforme mencionado em item anterior deste mesmo capítulo. Esta ferramenta tem seu funcionamento fundamentado nos descritores *MPEG-7* criados pelo *CALIPH*, e possibilita a recuperação das imagens por intermédio de texto (com a utilização de palavras-chave dos descritores), por consulta a nós de grafos semânticos armazenados ou ainda por similaridade das demais imagens do repositório com uma imagem previamente selecionada.

A implementação deste trabalho experimental fundamentou-se nas seguintes etapas:

1. Definição de uma listagem de músicas para a realização da anotação semântica; nesta etapa, foram selecionadas 10 músicas (cujos títulos não apresentam relação direta com palavras do refrão destas ou que não apresentam “letra cantada”).

2. Obtenção dos dados a serem anotados por intermédio do software de edição de áudio Audacity;

Nesta etapa, iniciou-se a utilização do Audacity, um software livre que se destina à captação, edição, gravação e análise de arquivos de áudio. Cada uma das músicas teve um intervalo selecionado, correspondente ao seu refrão ou à parte mais propícia a ser lembrada pela maioria dos usuários no momento de realização de uma consulta.

Após este procedimento, é realizada a análise do trecho de áudio. A análise é fundamentada na frequência atingida a cada variação de decibéis da música. O *Audacity* retorna o resultado desta análise graficamente, como é representado pela Figura 2, da próxima página. A realização da anotação semântica com o *CALIPH* utilizará, além da imagem deste gráfico, os dados referentes ao mesmo, contidos em um arquivo de texto simples, gerado pelo próprio *Audacity*, e denominado espectro de frequência.

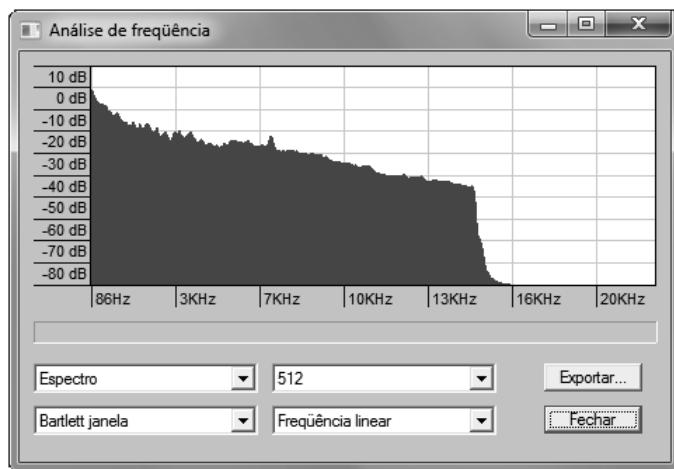


Figure 2. Gráfico gerado pelo *Audacity*, após a análise do intervalo selecionado de “*Bitter Sweet Symphony*”.

3. Realização da anotação semântica das músicas pertencentes à listagem por intermédio do *CALIPH*;

O *CALIPH* possui a interface desenvolvida propriamente para anotação semântica em arquivos de imagem. Ele é preparado para identificar, dentro de um diretório selecionado, somente arquivos com extensões de imagem. Considerando que a proposta de análise deste trabalho refere-se a arquivos de áudio, foi utilizada uma imagem para representar cada um destes, para que os mesmos pudessem ser anotados semanticamente. Para aumentar a eficiência da anotação semântica, foi utilizado como imagem, para cada um dos trechos, o seu respectivo gráfico de análise de frequência (gerado pelo *Audacity*).

4. Coleta do assvio de voluntários simulando um trecho musical referenciado na base de dados criada com o *CALIPH*;

A coleta de assvios de voluntários ocorreu de duas maneiras: presencialmente, com a utilização de um microfone acoplado ao fone de ouvido (*headset*) e por meio da

ferramenta de comunicação *on-line Skype*, com a utilização do meio de captação de voz pessoal de cada voluntário.

Para cada uma das músicas selecionadas, foi criado um arquivo denominado “Trecho nº de identificação da música”, contendo somente o intervalo correspondente ao refrão ou a alguma parte considerada marcante desta. A seguir, é apresentada a Tabela 1, próxima página, com as músicas e a nomenclatura de seus respectivos trechos, bem como a duração de cada um deles.

Tabela 1. Listagem das músicas e dos tempos de seus respectivos trechos selecionados para serem assoviados

<i>Música</i>	<i>Trecho</i>	<i>Duração (em segundos)</i>
<i>Bitter Sweet Symphony</i>	Trecho 1	23 s
<i>Blue Monday</i>	Trecho 2	17 s
<i>Enjoy the Silence</i>	Trecho 3	16 s
<i>Entre a cruz e a espada</i>	Trecho 4	20 s
<i>L'Aurora</i>	Trecho 5	19 s
<i>Losing my Religion</i>	Trecho 6	16 s
<i>Not Exactly</i>	Trecho 7	19 s
<i>The Rockafeller Skank</i>	Trecho 8	12 s
<i>Uma Brasileira</i>	Trecho 9	20 s
<i>Unchained Melody</i>	Trecho 10	20 s

O experimento foi realizado com cada participante individualmente. Foram, no total, 8 participantes (4 via *Skype* e 4 presencialmente), os quais somaram 21 amostras de assovios. A coleta de amostras realizada pelo *Skype* ocorreu do seguinte modo:

- Era enviado ao participante um arquivo compactado, denominado “Trechos.rar”.
- O participante era instruído a descompactar o arquivo, ouvir os dez trechos das músicas por uma vez, e selecionar o número de trechos que gostaria de assoviar.
- Após a escolha de quais trechos seriam assoviados, o participante poderia ouvi-los novamente, antes de iniciar o assvio correspondente ao trecho, pelo número de vezes que considerasse necessário.
- A gravação do assvio era então iniciada com um aplicativo adicional do *Skype*, denominado *Pamela Call Recorder*.

Presencialmente, o áudio era captado por um microfone acoplado a *headset* e gravado pelo *Audacity*.

5. A anotação dos arquivos de áudio captados dos participantes foi realizada seguindo a mesma sequência da anotação dos trechos das músicas.

5. Conclusões e Trabalhos Futuros

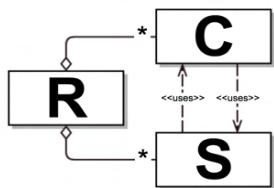
Dentre os 21 assóvios coletados, observou-se que a variação da relevância da consulta está fortemente conectada ao tipo de música assobiada e à maneira como o voluntário identifica o elemento principal da música. Nas imagens geradas pela análise dos trechos propostos para assobio foi realizada a anotação semântica com o *CALIPH*, contudo estas não foram indexadas na base de dados do *EMIR* para as consultas, devido a incompatibilidades com uma amostragem efetuada somente por assóviros. Estas incompatibilidades devem-se ao conjunto de instrumentos existentes e de elementos vocais adicionados eletronicamente nas músicas que não podem ser reproduzidos com um assobio. Este fator, no entanto, não representa a inviabilidade do método *QBH* ser realizado com o auxílio de um *software* de anotação semântica no processo de análise das consultas efetuadas. Foi identificada a necessidade de maior quantidade de amostras para cada música armazenada ou referenciada em um sistema com esta abordagem.

Como trabalhos futuros, podem ser propostos: a busca por um modo de otimização dos índices de relevância das consultas, com a utilização do padrão MPEG-21 para a produção de novos descritores; a ampliação da base de dados do *CALIPH*, sem interferência nos resultados satisfatórios obtidos; a realização de um paralelo entre uma nova base de dados anotada semanticamente por meio de outras características dos arquivos de áudio analisados; e a associação de outras opções de anotação do *CALIPH* e de outras opções de recuperação do *EMIR* para as amostras apresentadas .

Referências Bibliográficas

- AUDACITY (2003). Software de análise sonora. Revista Sonora, 4 (2), São Paulo: Abril.
- BARRIGTON, Luke; CHAN, Antoni, TURNBULL, Douglas; LANCKRIET, Gert (2007) Audio information retrieval using semantic similarity. Proceedings of the IEEE ICASSP, 32, p. II-725-II-728.
- DJERABA, Chabane; SEBE, Nicu; LEW, Michael S. (2005) Systems and Architectures for Multimedia Information Retrieval. ACM Multimedia Systems Journal. 10 (6), p. 457-463.
- ELMASRI, Ramez; NAVATHE, Sham (2007). Fundamentals of Database Systems. Boston: Pearson/Addison Wesley.
- FOOTE, Jonathan T. (1999) An overview of audio information retrieval. Multimedia Systems. 7 (1). 1, p. 2-11, ACM Press/Springer-Verlag.
- GAGLIARDI, Isabella; PAGLIARULO, Patrizia (2005) Audio Information Retrieval in Hypermedia Environment. In: ACM Conference on Hypertext and Hypermedia, 6, Salzburg.
- ISO/IEC TR 21000-1:2004 (2004). “Information technology – Multimedia framework (MPEG-21) – Part 1: Vision, Technologies and Strategy”, New York: ISO.
- KOSCH, Harald; DÖLLER, Mario (2005). Multimedia Database Systems: Where are we now? In: IASTED - INTERNATIONAL CONFERENCE ON DATABASES AND APPLICATIONS, Innsbruck.

- LEW, Michael S; SEBE, Nicu; DJERABA, Chabane; JAIN, Ramesh (2006). Content-based Multimedia Information Retrieval: State-of-the-art and Challenges. *ACM Transactions on Multimedia Computing, Communication, and Applications*. 2(1) p. 1-19.
- LAU, Edmond; DING, Annie; ON, Calvin (2010). MusicDB: A Query by Humming System. Massachusetts, 2007. Disponível em: <<http://people.csail.mit.edu/edmond/projects/musicdb/musicdb.pdf>>. Acesso em: 07 Nov. 2010.
- PEREIRA, Fernando; KOENEN, Rob (2010). MPEG: Context, Goals and Working Methodologies. Disponível em: <http://media.wiley.com/product_data/excerpt/18/04700101/0470010118.pdf> . Acesso em: 02 Set.2010.
- SONERA (s.d.) (2010). MPEG-7 White Paper,. Disponível em: <<http://www.medialab.sonera.fi/workspace/MPEG7WhitePaper.pdf>>. Acesso em: 02 Set.2010.
- TZANETAKIS, George; COOK, Perry (2000). Audio information retrieval (AIR) tools. Proceedings of the Annual International Symposium on Music Information Retrieval (ISMIR 2000), Los Angeles, p. 135-144.



Aplicação da Realidade Aumentada em Sessões de Fonoaudiologia para TEA: Um Estudo de Caso

Camilla Almeida da Silva¹, António Ramires Fernandes², Ana Grasielle D. Corrêa¹

¹Faculdade de Computação e Informática, Universidade Presbiteriana Mackenzie

²Departamento de Informática, Universidade do Minho.

camilla.sil@gmail.com, arf@di.uminho.pt, ana.correa@mackenzie.br

Abstract. The graphics systems of Augmented and Alternative Communication are widely used to promote communication of people with Autism Spectrum Disorders, however, there are studies that indicate the inability of some of these people in understanding the used symbols. This study discusses the integration of the use of Augmented Reality in communication interventions, by relating elements of strategies of Augmented and Alternative Communication and Applied Behavior Analysis to produce an interactive system to support interventions. A prototype was used in a case study to evaluate the proposed approach.

Resumo. Os sistemas gráficos de Comunicação Aumentativa e Alternativa são amplamente utilizados para promover a comunicação de pessoas com Transtornos do Espectro Autista, no entanto, há estudos que apontam a inabilidade de algumas dessas pessoas na compreensão dos símbolos utilizados. Este trabalho aborda a integração do uso da tecnologia da Realidade Aumentada em intervenções em comunicação, relacionando elementos de estratégias de Comunicação Aumentativa e Alternativa e Analise Comportamental Aplicada para elaborar um sistema interativo para apoio às intervenções. Um protótipo foi aplicado em um estudo de caso a fim de avaliar a abordagem proposta.

1. Introdução

As pessoas com Transtorno do Espectro Autista (TEA) apresentam comprometimentos em comunicação, sociabilização e imaginação, três áreas importantes do desenvolvimento. Em relação às dificuldades de comunicação, estas podem apresentar desde ausência total de linguagem até alteração na compreensão e pragmática da linguagem (PADILHA, 2008), com estimativas de que 50% das pessoas com TEA nunca chegam a desenvolver uma linguagem efetiva (SALLE et al., 2005), ressaltando a necessidade de criar meios para promover a comunicação para essas pessoas.

O programa de intervenção *Applied Behavior Analysis* (ABA) é eficaz para o ensino de novas habilidades e mudanças no comportamento, por meio de aprendizagem estruturada e utilização de reforços positivos e ajudas. As estratégias de Comunicação Aumentativa e Alternativa (CAA), em especial os sistemas gráficos, são as mais

utilizadas em intervenções em comunicação para crianças com TEA, assumindo grande importância na promoção da comunicação, redução de problemas comportamentais e auxiliar na compreensão do ambiente (NATIONAL RESEARCH COUNCIL, 2001).

O uso dos sistemas gráficos apoia-se nas características de forte processamento visual presente nos TEA, entretanto Herrera et al. (2012) acreditam que os comprometimentos na área da imaginação, caracterizados pela rigidez e inflexibilidade, podem causar dificuldades na compreensão dos símbolos utilizados. Os autores explicam que algumas pessoas com TEA enxergam nos símbolos apenas um conjunto de linhas, formas e cores e que o uso dos cartões de comunicação dar-se-ia pela memorização e associação ao contexto. Desta forma, concluem que os símbolos não fazem sentido para essas pessoas e, como evidência, citam que elas deixam de reconhecer um símbolo utilizado por simples modificações realizadas no desenho, como cor de fundo e espessura das linhas. O National Research Council (2001), a respeito disso, afirma que a capacidade simbólica é um dos défices fundamentais da comunicação e reflete a dificuldade de aprender o significado convencional ou compartilhado dos símbolos. Para serem utilizados nos processos comunicativos, os símbolos devem, primeiramente, fazer sentido ao sujeito (AVILA, 2011).

A Realidade Aumentada (RA), que combina objetos virtuais no ambiente real, pode ser explorada em diversas áreas de intervenções em TEA, como distinção de si próprio dos outros, comunicação aumentativa, consciência e identificação de emoções, dirigir a atenção para envolvimento social, conceito de permanência de objetos, compreensão de símbolos e desenvolvimento de conceitos (HERRERA et al., 2006). Considerando a importância das estratégias de CAA para crianças com TEA e o impacto que as dificuldades mencionadas teriam sobre a promoção da comunicação, buscou-se uma abordagem para integrar o uso da RA em intervenções em comunicação com crianças com TEA, relacionando elementos de estratégias de CAA e ABA para elaboração de um sistema interativo para apoio às intervenções, com a finalidade de amenizar a dificuldade de compreensão dos símbolos gráficos resultante de problemas de imaginação e simbolismo, característicos da rigidez de imaginação. Agregar informações aos cartões de comunicação auxiliará no processo de compreensão dos símbolos. Um cartão de comunicação referente a uma ação aumentada com um objeto virtual animado tornaria mais evidente o seu significado. O uso deste tipo de estratégias favorece o processo de aprendizagem, visto que autistas são “pensantes visuais”, conforme afirma Barbosa (2010), que diz que, no processo de informação, o primeiro sentido a ser estimulado é o visual devido a este ser o principal sentido no autista.

Desta forma, propôs-se um sistema com funcionalidades para elaboração de atividades a partir de *templates* pré-existentes, com enriquecimento dos cartões de comunicação com objetos virtuais 3D e áudio, adaptáveis às necessidades e características dos pacientes, incluindo recursos para seleção da forma de interação com as atividades, de comportamentos associados aos cartões de comunicação e, baseados em estratégias comportamentais, seleção e configuração de reforços sonoros e visuais. Outros recursos propostos no sistema foram: registro de desempenho; associação de perfis para automatizar a personalização das atividades a cada paciente; e treinamento a distância, com suporte a realização das atividades assistida pelo computador.

Na modelagem do sistema foram empregues instrumentos de coleta e análise do referencial teórico e dos dados coletados para definir o sistema a ser desenvolvido e

seus requisitos. Com base no referencial teórico, conduziram-se reuniões com especialistas para identificar as possíveis aplicações da RA nas intervenções com autistas, e caracterizar as atividades atualmente realizadas.

A fim de avaliar a abordagem proposta, desenvolveu-se um protótipo que foi aplicado em um estudo de caso com quatro crianças com TEA em sessões de fonoaudiologia. Seguiu-se, desta forma, o framework de Moore, D. et al. (2000) no qual é proposto que sistemas de aprendizagem assistida por computador para autista devam abordar ao menos um dos principais comprometimentos do TEA e que os projetos sejam fundamentados em práticas pedagógicas correntes e avaliados em colaboração com especialistas educacionais com bases cognitivas.

2. Transtorno do Espectro Autista

O TEA é um grupo de transtornos com causa desconhecida, afetando indivíduos de todas as raças e culturas.. Este grupo de transtornos é caracterizado por uma grande variabilidade tanto nos sintomas quanto no grau de acometimento, mas apresenta em comum uma interrupção precoce dos processos de sociabilização (KLIN, 2006). O comprometimento no desenvolvimento varia em grau, sendo uma condição que “é vista como um contínuo que vai do grau leve ao severo.” (PADILHA, 2008).

Os *Centers for Disease Control and Prevention* (2013) estima que existe em média 1 caso para cada 88 crianças nascidas nos Estados Unidos, sendo a incidência nos meninos quase cinco vezes maior que nas meninas. Também divulga que estudos na Ásia, Europa e América do Norte, identificaram indivíduos com uma prevalência aproximada 1%.

2.1. Intervenções

O objetivo principal das intervenções é minimizar as principais características do TEA, sendo as intervenções educacionais, incluindo estratégias comportamentais e terapias, os pilares do manejo do TEA (MYERS; JOHNSON, 2007). Os programas de intervenção requerem uma base multidisciplinar envolvendo terapias comportamentais, programas educacionais e terapias de linguagem/comunicação (GADIA et al., 2004).

A ABA é um processo de intervenções para a mudança sistemática do comportamento, objetivando aumentar e manter comportamentos desejáveis; reduzir os comportamentos indesejáveis, ou, restringir as condições em que eles ocorram; ensinar novas habilidades, comportamentos e generalizá-los a novos contextos (MYERS; JOHNSON, 2007). Os métodos ABA de duração limitada são eficazes para crianças e adultos com TEA (NATIONAL RESEARCH COUNCIL, 2001). A metodologia empregada na ABA é conhecida por Tentativas Discretas (DTT, sigla do inglês *Discrete Trial Teaching*) com foco em maximizar a aprendizagem é utilizado para desenvolver diversas capacidades, como cognição, comunicação e socialização (BARBOSA, 2010). Consiste em um método de aprendizagem estruturada que divide em passos pequenos de uma sequência complicada de aprendizagem, acompanhados de reforços positivos e ajudas conforme necessidade. (NETO et al., 2011).

A CAA é conceituada por Nunes e Nunes Sobrinho (2010) como “uma ampla variedade de métodos e técnicas que complementam ou substituem a linguagem oral comprometida ou ausente” e podem ser classificadas como “comunicação apoiada” e “comunicação não apoiadas” (MANZINI; DELIBERATO, 2006). A primeira trata das

estratégias em que a comunicação apoia-se em formas físicas e fora do corpo, como objetos reais, miniaturas, símbolos gráficos e sistemas computadorizados. A segunda refere-se a aquelas que englobam expressões próprias do indivíduo como gestos, linguagem de sinais, expressões faciais e movimentos do corpo. Desta forma a CAA, considerando as necessidades de cada pessoa, proporciona meios diversos para promover a comunicação e sua independência (AVILA, 2011).

Os métodos e ferramentas de intervenções com CAA são adaptáveis às características e necessidades das crianças autistas. Os sistemas gráficos de linguagem aproveitam o forte processamento visual de muitas das crianças autistas e vem se mostrando efetivo para aumentar a recepção de comunicação em crianças pequenas e para substituir comportamentos problemáticos, como agressão, autoagressão e choros, através do treinamento de comunicação funcional, também podendo ser utilizados para auxiliar a compreensão do ambiente através da estruturação do espaço e tempo.

O programa de treinamento comunicacional PECS, traduzido para o Português como Sistema de Comunicação por Troca de Figuras, é um método de CAA para ensino de comunicação funcional através da troca de imagens, desenvolvido por Bony e Frost em 1985. O método incorpora os princípios do ABA, baseando-se no Comportamento Verbal, e é composto por 6 fases cada qual com objetivos, configurações de ambiente, instruções e procedimentos de treinamento específicos. Nas fases iniciais, a criança é ensinada a iniciar pedidos através das figuras, passando a elaborar sentenças, responder a perguntas e fazer comentários já nas fases mais avançadas. (ALMEIDA et al., 2005; PECS, 2013). Bez (2010) cita alguns exemplos de estudos que apontam que o uso do PECS com crianças autistas resultaram em aquisição e aprimoramento da comunicação verbal e comunicação social e melhora no comportamento.

3. Trabalhos Correlatos

Herrera et al. (2012) desenvolveram o Pictogram Room, um sistema de RA para Microsoft Kinect, para ensinar as crianças sobre autoconsciência, esquema corporal e posturas, comunicação e imitação através de vários jogos educacionais relacionados ao corpo.

Tentori e Hayes (2010) propuseram o framework Mobile Social Compass para desenvolvimento de sistemas móveis de RA que possibilite o uso do The Social Compass, uma intervenção educacional e comportamental para grupos que faz uso de histórias e pistas visuais de papel para orientar a criança em interações sociais de forma ativa e passiva. O framework foca no conceito Interaction Immediacy proposto pelos autores, provendo um conjunto de dicas visuais para auxiliar a criança a antecipar situações. Escobedo et al. (2012) desenvolveram a aplicação MOSOCO, uma aplicação assistiva móvel que faz uso de RA e suportes visuais para auxiliar crianças com TEA a praticar habilidades sociais em situações de vida real. O sistema guia as crianças em seis habilidades sociais básicas do currículo The Social Compass encorajando-as através de recursos interativos. O resultado da análise do uso do sistema por três crianças autistas demonstrou que o sistema facilitou a prática e aprendizagem de habilidades sociais, aumentou a quantidade e qualidade das interações sociais, reduziu erros comportamentais e sociais e permitiu a integração social de crianças autistas em grupos com crianças neurotípicas.

Escobedo e Tentori (2011) visando amenizar as dificuldades de uma criança autista para se deslocar no ambiente escolar, propuseram o Blue's Clues, uma aplicação móvel de RA que provê dicas audiovisuais para orientar a criança na direção correta e também dispõe de um módulo em que permite a um responsável verificar a localização da criança no mapa.

4. Protótipo

Desenvolveu-se um protótipo com um conjunto de funcionalidades básicas necessárias para avaliar a abordagem proposta em um estudo de caso. Por meio desse protótipo, podem ser criadas atividades interativas com recursos de RA e apoiada em estratégias de CAA e ABA. As atividades podem ser elaboradas a partir de *templates* e contam com parametrização de reforços audiovisuais, gerenciamento de erros, formas de interação e comportamento do sistema aquando da interação com os marcadores.

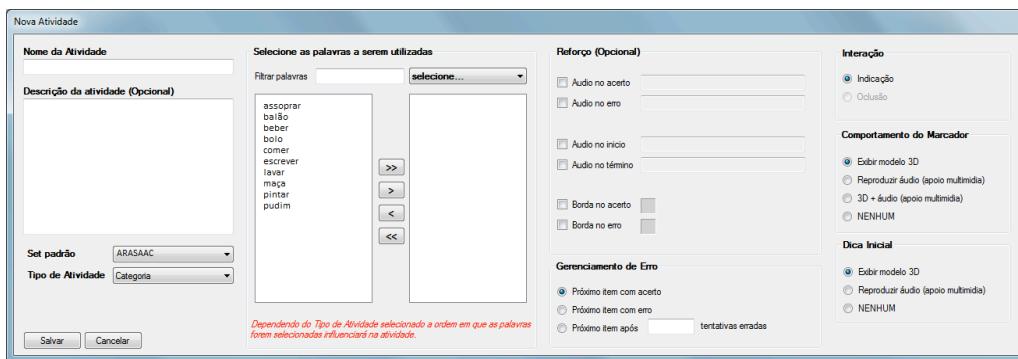


Figura 1. Interface para elaboração de atividades.

O protótipo foi implementado recorrendo a bibliotecas públicas de software, nomeadamente irrKlang para áudio, ARToolkit para a componente de RA, e MySQL. A escolha deste ambiente visou priorizar um sistema de baixo custo de produção e aquisição, e com suporte multiplataforma para portabilidade futura.

O ambiente é formado pelo usuário – paciente conduzido pelo terapeuta –, a aplicação de RA (atividade), um computador, um dispositivo de captura de vídeo (*webcam*), um dispositivo de visualização (monitor) e marcadores.

O funcionamento básico das atividades consiste em exibir um marcador no campo de visão da *webcam* que, de acordo com a forma como foi configurado o seu comportamento, poderá exibir o objeto virtual e reproduzir o áudio correspondente. Os *templates* disponíveis são: *Livre*, *Frase*, *Discriminar* e *Categoria*.

No *template Livre* o usuário poderá interagir livremente com o sistema exibindo o marcador desejado para acionar o seu comportamento. Este *template* permite parametrizar reforços positivos, forma de interação e comportamento. Adicionalmente, quando selecionada a forma de interação por oclusão, é possível configurar um comportamento para quando o marcador é ocultado. Um exemplo de elaboração de atividade com interação por oclusão seria configurar o comportamento de interação para exibir o objeto virtual 3D e o comportamento de oclusão para reproduzir o áudio. Supondo que a atividade tenha sido elaborada com animais, ao inicio da atividade o usuário visualizaria sobre cada marcador a representação 3D de um animal e, ao ocultá-lo, seria reproduzido o som deste animal.

No *template Frase* o usuário terá que colocar os marcadores de modo a formar a frase previamente estipulada. A cada marcador poderão ser acionados reforços, positivos e negativos, para indicar se o marcador é o correto e se está na ordem correta. O sistema permite ainda definir reforços para quando a sequência está correta. Através dos reforços, espera-se que a criança compreenda mais facilmente a importância da ordem dos cartões de comunicação para passar a mensagem desejada.

O funcionamento dos *templates Discriminar* e *Categoria* consiste em exibir uma dica de um símbolo, por exemplo, um objeto 3D e/ou áudio. Perante o marcador exibido poderão ser acionados reforços positivos ou negativos. Um marcador especial é empregado com a função de exibir a dica do símbolo corrente ou passar para o próximo símbolo. Esse *template* possui um gerenciamento de erro que pode ser configurado para permitir que o marcador especial passe para o próximo símbolo apenas se o usuário tiver acertado o anterior, ou, mesmo tendo errado o símbolo anterior, podendo ser determinado a quantidade de tentativas mínimas.

As opções variadas de tipos de atividades, através de *templates*, buscou evitar a tendência de repetição de mesmas tarefas pelo autista. Os *templates* propostos baseiam-se nas fases I, III e IV do PECS.

5. Avaliação

O Estudo de Caso desenvolveu-se com o apoio de uma instituição de apoio ao TEA localizada em Braga, Portugal, consistindo-se da utilização e análise do *software* por fonoaudióloga com experiência no trabalho com autistas, permitindo avaliar o sistema e identificar seus benefícios. Realizaram-se sete sessões entre os meses de maio e julho com quatro meninos entre 6 e 10 anos diagnosticado com TEA. Todos os sujeitos apresentam algum nível de oralidade e frequentam o ensino regular ou estruturado. Alguns dos sujeitos são caracterizados como participativos nas sessões de fonoaudiologias, enquanto outros são ditos extremamente passíveis em termos de comunicação e comportamento. Um dos sujeitos apresenta várias estereotipias verbais e motoras e um discurso maioritariamente constituído por ecolalias.

Adotou-se uma investigação qualitativa caracterizada por um estudo de caso com recolha de dados através de observação participante, tal estratégia adequou-se à necessidade de observar e compreender o comportamento das crianças face à utilização do software. Para apoio a recolha de dados, realizaram-se registros de vídeos das sessões e, como instrumento de observação, foram confeccionadas grelhas de observação, um recurso frequentemente utilizado em estudos com múltiplos sujeitos.



Figura 2. Interações com o software.

As crianças demonstravam iniciativa em realizar as atividades, como o ato de apontar para os materiais utilizados no início da sessão demonstrando interesse em

jogar. Outra situação que apresentam indícios do interesse pela atividade, foi um pedido realizado por “B”, um menino com diversas estereotipias verbais e motoras e que passa toda a sessão solicitando para ir à janela para avistar automóveis e repetindo frases descontextualizadas. “B” pediu pelo marcador do cachorro à terapeuta após ela ter recolhido os materiais e avisado que iniciariam outro tipo de atividade, em posse do marcador, mostrou-o autonomamente ao computador, exibindo uma expressão de alegria ao ouvir o som reproduzido. “C”, definido pela terapeuta como uma criança passiva em termos de comunicação e comportamento, durante as atividades realizadas motivava-se em repetir o que era reproduzido pelo computador, bem como “corrigir o computador” quando de um erro de reconhecimento.

Ao término da avaliação, a fonoaudióloga emitiu um relatório sobre as sessões, destacando suas impressões a respeito do uso do sistema. Sobre os aspectos positivos, a terapeuta destacou o fato das crianças se manterem atentas e interessadas na realização das tarefas, inclusive demonstrarem iniciativa para utilização do software. Relata também que observou algumas aquisições e uma consistência em termos de realização bem sucedida das tarefas. No entanto, a terapeuta refere também que o contato ocular ocorre menos vezes assim como a atenção partilhada diminui, em particular no caso de uma das crianças que “desligava-se” do mundo a sua volta, a sua atenção fixa em sua imagem na tela de captura de vídeo.

5.1. Estratégias

Os objetivos traçados pela terapeuta da fala para a utilização do protótipo foram delineados de acordo com o plano de intervenção já traçado para cada criança e adaptado às possibilidades do programa.

Para três crianças foram traçados os seguintes objetivos: (1) Identificar animais, alimentos e objetos do quotidiano; (2) Identificar e nomear gênero; (3) Identificar e nomear ações; (4) Discriminar e identificar sons ouvidos; (5) Responder afirmativamente e negativamente oralmente, associado ao movimento da cabeça; e (6) Construir sentenças com sujeito, verbo e objeto com apoio dos símbolos do sistema gráfico ARASAAC.

Para uma das crianças os objetivos foram: (1) Desenvolver a função declarativa; (2) Melhorar competências discursivas com apoio dos objetos 3D para estruturar a informação de maneira adequada, assim como respeitar a tomada de vez e temática; (3) Criar e imaginar sobre a linguagem.

Elaboraram-se seis atividades com base nos *templates Categoría, Discriminar, Frase e Livre* para atingir os objetivos propostos e os materiais utilizados pela terapeuta foram os marcadores com símbolos do sistema gráfico ARASAAC, canudos que foram afixados aos marcadores para auxiliar no manuseio e figuras com fotos retratando as situações para apoio às atividades do tipo Frase.

6. Conclusões

Os resultados demonstraram que o emprego do *software* em intervenções em comunicação, complementando e apoiando as metodologias tradicionais, é uma opção a explorar.

O estudo levantou indícios de que a utilização do software poderá ser uma mais valia para as intervenções em comunicação, no sentido de que, além de observar ganhos na motivação, interesse e iniciativa, também foram observadas aquisições e consistência nos acertos e em respostas do tipo “sim/não”, conforme considerações da terapeuta. O trabalho realizado apresenta potencial para se utilizar no trabalho de competências linguísticas, assim como se observam benefícios no aumento de iniciativa comunicativa por parte da criança.

A utilização deste tipo de software pode por outro lado implicar, em certos casos, o perigo da negligência da interação social, sendo necessário um cuidado extra por parte dos terapeutas para detectar e/ou evitar estas situações.

As atividades mostraram-se de fácil compreensão, atribuindo-se isso ao uso de interfaces tangíveis através dos cartões de comunicação, um material comum às crianças, pois foram aproveitadas as experiências e habilidades das crianças, já que a interação com o computador tornou-se semelhante ao praticado em estratégias de CAA, que se fundamentam na troca de cartões de comunicação entre paciente e terapeuta. Indo ao encontro do sugerido por Billinghurst et al. (2005 apud TORI et al., 2007), que afirmam que para que o uso da interface tangível seja intuitiva e natural, é necessário a escolha de objetos físicos e metáforas comuns aos usuários, permitindo que eles baseiem-se em suas habilidades e experiências. A escolha da RA como tecnologia subjacente visou: (1) prover um meio natural para interação com o computador; (2) facilitar a generalização do que vier a ser aprendido com apoio do sistema; e (3) diminuir a possibilidade de distrações e dificuldades de manuseio, como ocorre com o uso de interfaces comuns como o *mouse* e teclado.

Acredita-se que os resultados positivos observados neste estudo devam-se pelo ambiente interessante e motivador de aprendizagem propiciado pelo *software*, devido ao seu caráter interativo e multissensorial, que estimula o processamento cognitivo e leva a uma aprendizagem visual. Os recursos de interação, animação e áudio apreendeu a atenção das crianças como sugerido em diversos estudos sobre o benefício das TIC em intervenções com crianças com TEA (MOORE, M.; CALVERT, 2000; MOORE, D. et al., 2000; KOVATLI, 2003; GOLDSMITH; LEBLANC, 2004). Também se atribui os resultados ao uso de interfaces tangíveis, que como sugerido por Farr et al. (2009) podem apoiar as crianças com TEA a colaborar e comunicar numa nova maneira e por um tempo maior, promovendo assim maior interação.

6.1. Trabalho Futuro

Os resultados obtidos reforçam a necessidade em dar continuidade a esta proposta, prosseguindo com novas iterações e testes, cujo sucesso requer uma equipe multidisciplinar para possibilitar uma maior abrangência da solução.

Relativamente ao uso do *software*, sentiu-se necessidade de adicionar mais *templates* e configurações, por exemplo, com níveis de dificuldade na construção de frases. Também se faz necessário atentar-se ao reconhecimento e identificação dos marcadores, pois houve uma quantidade significante de falhas no rastreamento. No estudo realizado, tais falhas não prejudicaram as crianças participantes, pois foram exploradas pela terapeuta que as tornou parte das atividades, entretanto deve-se garantir as respostas consistentes e previsíveis para propiciar um ambiente estruturado.

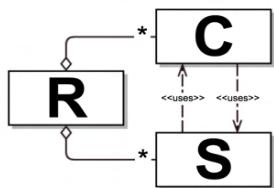
Dado aos limites do estudo realizado em relação ao tempo e a quantidade de sujeitos participantes que não refletem a grande variedade de perfis autistas, justifica-se a necessidade de realizar novos estudos para avaliar se os resultados aqui obtidos podem ser generalizáveis, principalmente quanto ao desenvolvimento das habilidades de comunicação e linguagem por meio de aquisições de vocabulário (apropriação do significado dos símbolos do cartão de comunicação).

Referências

- ALMEIDA, M. et al. Adaptações do sistema de comunicação por troca de figuras no contexto escolar. *Pró-Fono Revista de Atualização Científica*, v. 17, n. 2, p. 233-240, 2005.
- AVILA, B. G. *Comunicação Aumentativa e Alternativa para o Desenvolvimento da Oralidade de Pessoas com Autismo*. 2011. Dissertação (Mestrado em Educação)-Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011.
- BARBOSA, H. F. A. *Análise do recurso a novas tecnologias no ensino de autistas*. 2010. Dissertação (Mestrado em Engenharia Informática – Sistemas Gráficos e Multimédia)-Instituto Superior de Engenharia do Porto, Porto, 2010.
- BEZ, M. R. *Comunicação aumentativa e alternativa para sujeitos com transtornos globais do desenvolvimento na promoção da expressão e intencionalidade por meio de ações mediadoras*. 2010. Dissertação (Mestrado em Educação)-Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010.
- Center for Disease Control and Prevention. *Autism Spectrum Disorder*. Disponível em: <<http://www.cdc.gov/ncbdd/autism/data.html>>. Acesso em: 07 out 2013.
- ESCOBEDO, L. et al. MOSOCO: A Mobile Assistive Tool to Support Children with Autism Practicing Social Skills in Real-Life Situations. In: Conference on Human Factors in Computing Systems, 2012, Austin. *CHI '12 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM Press, 2012. p. 2589-2598.
- ESCOBEDO, L.; TENTORI, M. Blue's Clues: An Augmented Reality Positioning System. In: Conference on Human Factors in Computing Systems, 2011, Vancouver. *Child Computer Interaction Workshop*. New York: ACM Press, 2011. p. 1-4.
- FARR, W. et al. Collaborative Benefits of a Tangible Interface for Autistic Children. In: Conference on Human Factors in Computing Systems, 2009, Boston. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM, 2009. p. 1-4.
- HERRERA, G. et al. Exploring the advantages of Augmented Reality for Intervention in ASD. In: World Autism Congress. Cape Town: 2006.
- HERRERA, G. et al. Pictogram Room: Natural Interaction Technologies to Aid in the Development of Children with Autism. *Anuario de Psicología Clínica y de la Salud*, v. 8, 2012. p. 39-44.
- GADIA, C. et al.; ROTTA, N. Autismo e doenças invasivas de desenvolvimento. *Jornal de Pediatria. (Rio de Janeiro)*, Porto Alegre, v. 80, n. 2, supl. 0. abr. 2004, p. 83-94.

- GOLDSMITH, T.; LEBLANC, L. Use of Technology in Interventions for Children with Autism. *Journal of Early and Intensive Behavior Intervention*, v. 1, n. 2, p. 166-178, 2004.
- KLIN, A. *Autismo e Síndrome de Asperger: uma visão geral*. *Revista Brasileira de Psiquiatria*, São Paulo, v. 28, n. 1, 2006, p. S3-S11.
- KOVATLI, M. *Estratégias para estabelecer interação de crianças com autismo e o computador*. 2003. Dissertação (Mestrado em Ciência da Computação)-Universidade Federal de Santa Catarina, Florianópolis, 2003.
- MANZINI, E.; DELIBERATO, D. *Portal de ajudas técnicas para educação: equipamento e material pedagógico especial para educação, capacitação e recreação da pessoa com deficiência física: Recursos para comunicação alternativa*. 2. ed. Brasília: MEC, SEESP, 2006.
- MOORE, M.; CALVERT, S. *Brief Report: Vocabulary Acquisition for Children with Autism: Teacher or Computer Instruction*. *Journal of autism and developmental disorders*, v. 30, n. 4, ago. 2000. p. 359-362.
- MOORE, D. et al. *Computer-Aided Learning for People with Autism: a Framework for Research and Development*. *Innovations in Education & Training International*, v. 37, n. 3, jan. 2000. p. 218-228.
- MYERS, S.; JOHNSON, C. Management of Children with Autism Spectrum Disorders. *Pediatrics*, v. 120, n. 5, nov. 2007. p. 1162-1182.
- NATIONAL RESEARCH COUNCIL. Educating children with autism. 1 ed. Washington: National Academies Press, 2001.
- NETO, O. et al. *e-kids: Uma Ferramenta no Auxílio da Aprendizagem de Crianças Portadoras de Disfunção Global do Desenvolvimento (Autista), baseada no método ABA*. In: WIM WI Workshop de Informática Médica, 2011, Natal. *Anais... Natal: SBC*, 2011. p. 1-4.
- NUNES, D.; NUNES SOBRINHO, F. *Comunicação alternativa e ampliada para educandos com autismo: considerações metodológicas*. *Revista Brasileira de Educação Especial*, Marilia, v. 16, n. 2, mai-ago. 2010. p. 297-312.
- PADILHA, M. A Musicoterapia no Tratamento de Crianças com Perturbação do Espectro do Autismo, 2008. Dissertação (Mestrado Integrado em Medicina)-Universidade da Beira Interior, Covilhã, 2008.
- PECS. *O que é PECS?* Disponível em: <<http://www.pecs-brazil.com/pecs.php>>. Acesso em: 09 out 2013.
- SALLE, E. et al. *AUTISMO INFANTIL: SINAIS E SINTOMAS*. In: CAMARGOS JR., W. (Org.). *Transtornos Invasivos do Desenvolvimento: 3º Milênio*. 2 ed. Brasília: Presidência da República, Secretaria Especial dos Direitos Humanos, Coordenadoria Nacional para Integração da Pessoa Portadora de Deficiência, 2005.
- TENTORI, M.; HAYES, G. Designing for Interaction Immediacy to Enhance Social Skills of Children with Autism. In: Ubiquitous Computing, 2010, Copenhagen. *Ubicomp '10 Proceedings of the 12th ACM international conference on Ubiquitous computing*. New York: ACM Press, 2010. p. 51-60.

TORI, R. et al. Jogos e Entretenimento com Realidade Virtual e Aumentada. In: KIRNER, C.; SISCOUTTO, R. (Org.). *Realidade Virtual e Aumentada: Conceitos, Projeto e Aplicações*. Livro do pré-simpósio, IX Symposium on Virtual and Augmented Reality. Porto Alegre: Editora SBC, 2007. p. 192-222.



Avaliando Perfil de Disciplinas e Alunos com Mineração de Dados

Leandro Augusto da Silva

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie –
Rua da Consolação, 930 - 01302-907 – São Paulo – SP – Brasil

leandroaugusto.silva@mackenzie.br

Abstract. This paper addresses a data mining methodology with clustering analysis to categorize subjects from Information Systems courses. The database used was obtained by the students that are in the 6 semester of course, where they completed a spreadsheet with the final averages for each subject. The process used to find the groups was discussed and the results allow us to analyze the student profile, the outline course and to list the subjects in each group discovered. The presented results can be useful as indicator parameters, action planning, and also to support future works on the courses performance evaluations in educational.

Resumo. Este artigo apresenta uma metodologia de mineração de dados com técnica de agrupamento para categorizar disciplinas de um curso de Sistemas de Informação. Os dados utilizados foram conseguidos por meio de pesquisa aos alunos que estão no 6º Semestre do curso, onde os mesmos preencheram uma planilha com suas médias finais em cada disciplina. Todo o processo para descobrir os grupos foi discutido e os resultados encontrados permitem analisar o perfil dos alunos, o perfil do curso e relacionar disciplinas de cada grupo descoberto. Os resultados apresentados podem ter utilidade como construção de indicadores, planejamento de ações e, também, subsidiar trabalhos futuros sobre o desempenho de cursos em instituições de ensino.

1. Introdução

Um banco de dados constitui de uma estrutura para armazenamento de fatos que se relacionam de forma a fazer sentido. A chegada dos Sistemas Gerenciadores de Banco de Dados (SGBDs) trouxe, entre outras coisas, um armazenamento relacionado para eliminar redundâncias e aumentar a capacidade de armazenamento; uma coleção de restrições para garantir consistência no armazenamento dos dados e um conjunto de álgebras para possibilitar a construção de linguagens de consultas padronizadas. Podemos atribuir a esse fato, ocorrido por volta dos anos 80, como um dos principais propulsores para o desenvolvimento dos Sistemas de Informação (SI) [Silberchatz, Korth e Sudarshan, 2006].

A área profissional que atua em um SI é chamada de Tecnologia da Informação (TI) e por muito tempo tinha como principal desafio a sistematização de processos e uso de

SGBDs para o armazenamento de dados. Com a maturidade de linguagens de consulta estruturada ou SQL (do inglês, *Structured Query Language*), baseada em álgebras relacionais e teorias de conjuntos, os dados passam a ser manipulados, de tal maneira que seja possível construir relatórios estatísticos e, por conseguinte, os gestores passaram a vislumbrar esses resultados como apoio a tomadas de decisões.

Em paralelo a tudo isso, o hardware que antes era de dimensão reduzida em número de bytes e muito caro, evolui para um cenário totalmente oposto. E assim, começou a gerar grande volume de dados e o interesse por uma segunda geração de análise de dados, conhecida por Mineração de Dados ou DM (do inglês, *Data Mining*). O DM é parte de um processo que tem como entrada uma base de dados e como saída um conhecimento que estava intrínseco aos dados. Esse processo ficou conhecido por Descoberta de Conhecimento em Banco de Dados ou KDD (do inglês, *Knowledge Discovery Database*) [Fayyad et al., 1996], [Witten et al. 2011].

Não diferente das grandes corporações empresariais, as Instituições de Ensino, em geral, nas quais se incluem as de Ensino Superior (IES), tem grande parte das transações diárias armazenada em banco de dados. A cada dia estes dados são atualizados, como, por exemplo, no preenchimento das listas de presença, lançamento de notas de provas parciais, pagamentos de mensalidade, transferência de alunos e etc. Com o uso da linguagem SQL as IES também geram uma série de relatórios estatísticos, como, por exemplo, levantamento sobre ausências de alunos, médias parciais do semestre, levantamentos de aprovação de alunos, disciplinas com maior número de reprovação e muitas outras informações que auxiliam os gestores e coordenadores no acompanhamento de disciplinas, alunos e infra-estrutura de uma IES.

No entanto, estes levantamentos típicos são extrações triviais de dados que nem sempre permitem uma compreensão mais aprofundada e fundamentada para tomada de decisões. Além do mais, acredita-se que muitas outras informações estão escondidas nos grandes volumes de dados o que, consequentemente, poderiam ser úteis para apoiarem gestores em diversas esferas estratégicas na tomada de decisão. E nesse momento que se faz necessário o uso da DM.

DM é uma área interdisciplinar que envolve, basicamente, banco de dados, estatística e inteligência computacional e se aplica em várias áreas do conhecimento para descoberta de informações escondidas em bancos de dados [Fayyad et al., 1996].

Na área de educação, há na literatura muitas propostas de trabalhos usando Mineração de Dados [Pimentel e Omar, 2006; Dias et al., 2008; Romero e Ventura 2007; Romero e Ventura 2008; Marinho, Dermeval e Ferreira, 2009; Romero e Ventura 2010; Malvezzi, Mourão e Bressan, 2010]. Esta é uma área de interesse conhecida como Mineração de Dados Educacionais ou EDM (do inglês, *Educational Data Mining*) [Romero e Ventura, 2007; Romero e Ventura, 2010]. Segundo Romero e Ventura [2010], os tipos de estudos em EDM são classificados em:

- Educação presencial (*Offline education*): analisa os alunos com dados adquiridos a partir do seu comportamento em sala de aula, desempenho nas avaliações, *curriculum* e etc. Pode ser considerado como exemplo deste tipo de estudo, quando se deseja saber com antecedência o conhecimento do aluno em uma disciplina, a partir de uma avaliação prévia [Pimentel e Omar, 2006; Romero e Ventura 2007; Romero e Ventura 2010];

- Educação à distância e Sistema para gerenciamento de aprendizagem ou LMS (do inglês, *Learning Management System*) constitui-se da forma mais simples de fazer mineração de dados, pois o ambiente permite armazenar muitos parâmetros dos alunos como tempo de: estudo, leitura, resolução de exercícios e etc; desempenho em: exercícios, avaliação e etc; entre outros [Dias et al., 2008; Romero e Ventura 2008; Romero e Ventura 2010; Malvezzi, Mourão e Bressan, 2010];
- Sistemas tutores inteligentes ou ITS (em inglês *Intelligent Tutoring System*) e Sistemas hipermídia educacionais adaptativos ou AEHS (do inglês *Adaptive Educational Hypermedia System*) onde a mineração de dados é utilizada para adaptar os sistemas de ensino para cada perfil de estudante, usando como fonte de dados os arquivos de *log* do usuário, modelo de alunos, etc, os quais permitem fazer sugestões de estudos, ajuste de conteúdos e etc [Romero e Ventura 2007; Marinho, Dermeval e Ferreira, 2009; Romero e Ventura 2010].

Diane o contexto previamente apresentado, este trabalho tem como dois principais objetivos. O primeiro é contextualizar o processo de KDD em um problema real, discutindo a importância de cada fase do processo, servindo assim como um estudo de caso em EDM na classe de Educação presencial. O segundo e mais importante objetivo é usar notas de alunos cursando o 6º Semestre em Sistemas de Informação e, através da técnica de mineração de dados de análise de grupos, descobrir três diferentes padrões de disciplinas. Cada padrão será chamado de: difícil, regular e fácil. O algoritmo de agrupamento utilizado será o *k*-Médias, que de forma iterativa, particiona a base de dados em *k* distintos grupos [Witten et al. 2011]. Para a realização dos experimentos, utilizaremos a ferramenta *Rapid Miner*, disponível para download sem a necessidade de licença [Mierswa et al. 2006]. A principal novidade deste trabalho é que ao invés de avaliar o perfil do aluno, como em outros trabalhos da literatura [Romero e Ventura 2008; Romero e Ventura 2010], queremos aqui avaliar o perfil das disciplinas. Portanto, uma base de dados que, geralmente é organizada em exemplos (linhas) com alunos e atributos (colunas) com disciplinas, tendo como valor as notas tiradas, para permitir o estudo proposto neste trabalho, ela deverá passar por um rotaciomento, trocando as linhas por colunas.

Além da Introdução, que tem o objetivo de contextualizar a problemática estudada no trabalho e, apresentar o objetivo do trabalho, o artigo está organizado como segue. Na Seção 2 apresenta-se, de forma breve, uma introdução sobre mineração de dados e o processo de descoberta de conhecimento em bases de dados. Na seção 3 apresenta-se a metodologia adotada neste estudo. Na seção 4, os resultados obtidos e analisados são apresentados. Por fim, na seção 5, as discussões finais e conclusões prévias são apresentadas.

2. Mineração de Dados como um processo

Como se pode observar a partir da Figura 1, Mineração de Dados ou DM (do inglês, *Data Mining*) é parte de um processo maior chamado Descoberta de Conhecimento em Base de Dados ou KDD (do inglês, *Knowledge Discovery Database*).

No processo de KDD, cada fase deve ser avaliada em relação à necessidade, a partir do problema a ser resolvido. E também, cada fase pode ser repensada, em caso no passo

seguinte do processo uma tarefa anterior seja necessária. Ou seja, o processo é iterativo e interativo.

De forma breve, cada etapa do processo é definida como:

- Limpeza e integração: os dados, oriundos de uma ou mais bases, são integrados em um repositório único. Nesse processo, valores faltantes (*missing values*) e ou fora de um padrão (*outlier*) pode surgir na base de dados;
- Pré-processamento: alguns exemplos da base (linhas) ou atributos (colunas) são mais representativos que outros no processo de KDD e deve se pensar em manter ou em eliminar para a redução de complexidade na etapa do DM;
- Transformação: para que os dados estejam em um único formato, muitas vezes é preciso que se faça a normalização dos dados para que os valores fiquem em uma única escala de valor;
- Mineração de Dados ou DM: decide-se pela técnica de mineração a ser aplicada, de acordo com o problema em análise. Estas técnicas, de forma breve, podem ser definidas como:
 - Predição: consiste em mapear um exemplo desconhecido da base de dados, também chamada de base de treinamento, em um atributo especial chamado de rótulo (ou *label*, em inglês). Pode ser dividida em classificação (mapeamento em rótulos com valores discretos) e estimativa (mapeamento em rótulos com valores contínuos).
 - Agrupamento: consiste em agrupar os exemplos da base de dados que são similares entre si e dissimilares entre os grupos.
 - Associação de dados: consiste em encontrar relações entre atributos da base de dados.
- Interpretação ou avaliação dos resultados: os resultados de todo o processo precisam ser avaliados, em termos de desempenho, para que seja feita uma análise qualitativa (interpretação) ou quantitativa (avaliação) dos resultados obtidos

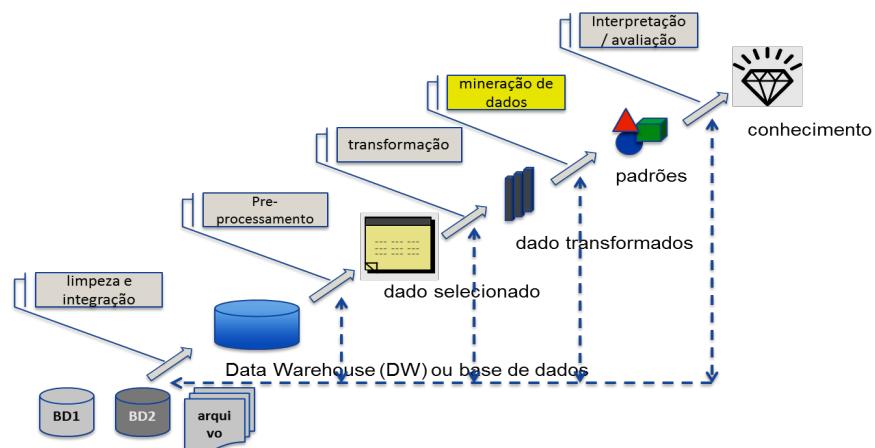


Figura 1. Processo de KDD no qual se inclui a Mineração de Dados [Fayyad et al. 1996].

2.1 Análise de agrupamento

Análise de agrupamento, como brevemente definido anteriormente, é uma técnica de mineração de dados usada para segmentar uma base de dados em grupos. Na literatura encontramos várias abordagens para descoberta de grupos em base de dados, como por exemplo, particionais, hierárquicas ou por grafo (para uma leitura completa sobre estas abordagens consulte [Witten et al. 2011]). Neste trabalho a escolha foi pela abordagem particional. Dentro dessa, a técnica utilizada foi a popularmente conhecida como *k*-Médias (ou *k-Means*) [Witten et al. 2011].

O algoritmo do *k* -Médias opera para gerar um particionamento da base de dados em *k* inteiros grupos da seguinte maneira:

```
Escolha k grupos aleatoriamente  
Calcule a centroide para cada grupo  
Repita  
    Atribua cada exemplo da base ao centroide mais próximo  
    Recalcule o centroide para cada grupo  
Até estabilidade
```

O valor de *k* e a métrica de distância são dois parâmetros que devem ser fornecidos à priori para o algoritmo *k*-Médias.

A escolha do valor de *k* pode ser um grande desafio para a aplicação do algoritmo. Em contextos onde se sabe previamente o número de grupos desejado, como neste trabalho, a escolha do parâmetro *k* é um problema trivial. Por outro lado, quando não se sabe o número de grupos ou, então, quando se deseja descobrir o número de grupos, é preciso considerar a variação do parâmetro e o uso de medidas quantitativas para que se faça a melhor escolha.

Entretanto, a escolha do outro parâmetro do algoritmo, métrica de distância, é um problema de menor proporção. Por consenso, é comum que se adote a distância Euclidiana. Contudo, há várias outras métricas que se pode utilizar como distância de Manhattan, distância do cosseno dentre outras [Witten et al. 2011]. O *Rapid Miner* permite a escolha dessas métricas de distância e de muitas outras [Mierswa et al. 2006].

Na próxima seção, a metodologia usada neste trabalho é apresentada e, com ela, uma discussão prática das fases do processo de descoberta de conhecimento será contextualizada, a partir do estudo de caso que o artigo apresenta.

3. Metodologia

Como introduzido previamente, os experimentos deste trabalho serão feitos com o uso da ferramenta de mineração de dados chamada *Rapid Miner* [Mierswa et al. 2006]. Trata-se de uma ferramenta de aprendizado simples, onde todas as fases da descoberta de conhecimento em bases de dados podem ser preparadas na forma de um processo, veja Figura 2. Note que, de todas as etapas do processo de KDD apresentado na Figura 1, apenas a transformação de dados não se fez necessário para o objetivo deste trabalho. Isso devido ao fato de todas as notas estarem em um intervalo de valores de 0 a 10.

Para a formação da base de dados, cada um dos 50 alunos cursando o 6º. Semestre em Sistemas de Informação recebeu uma planilha, exemplificada na Tabela 1. O aluno, sem se identificar, preencheu sua média final em todas as disciplinas cursadas até o corrente

período. Como resultado de preenchimento da planilha gerou-se uma base de dados com 50 exemplos (linhas) representando cada aluno e 39 atributos (colunas) representando as disciplinas oferecidas nos cinco primeiros semestres do curso.

Os alunos que tinham dependência foram orientados a preencher a planilha com a média final que tirou na primeira vez que cursou a disciplina.

Depois de finalizada a etapa de integração de todas as planilhas, observou-se que algumas notas não foram preenchidas. Isso se deve ao fato que na IES onde a pesquisa foi realizada, o aluno pode optar em montar a sua grade de disciplinas. Portanto, a base apresenta valores ausentes, em razão do aluno ainda não ter feito à disciplina, e que devem ser tratados pela limpeza.

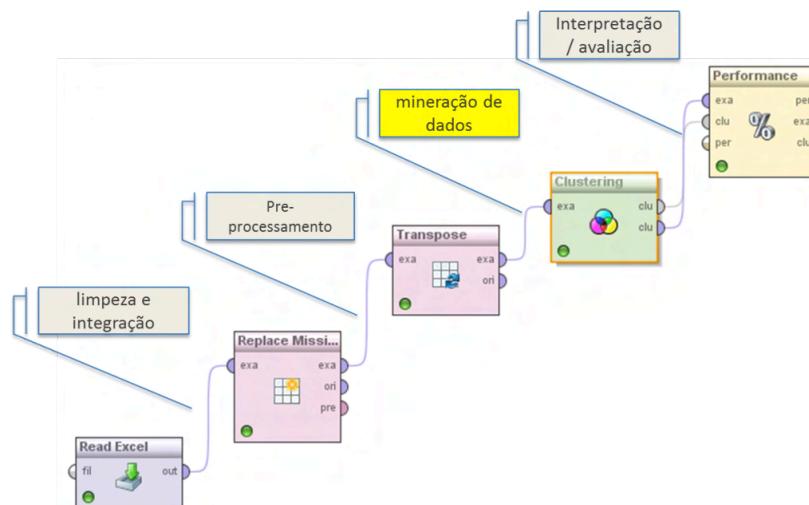


Figura 2. Processo empregado no trabalho para a segmentação da base de dados.

Tabela 1. Exemplo da planilha que cada aluno recebeu para preenchimento.

	1 Sem.			2º. Sem.			5º. Sem.		
	Ing. Téc. I	Mat.	...	Est. de Dados	Tec. Web.	...		Pesq. Opera.	Banco Dados	...
1	7,0	5,5	...	6,0	4,8	...		5,0	6,5	...
...
50	6,5	5,0	...	4,5	6,0	...		5,5	6,0	...

Para a realização da limpeza de preenchimento de valores ausentes, a ferramenta *Rapid Miner* oferece as seguintes opções: mínimo, média, máximo e nulo. A opção escolhida no projeto foi pelo valor mínimo, isto significa que as notas faltantes em alguma disciplina foram consultadas e escolheu-se para preenchimento àquela de menor valor. Esta etapa foi necessária para 1,5% de todos os valores da base de dados.

Como o objetivo do trabalho é identificar o perfil de cada disciplina, ou seja, verificar as disciplinas que os alunos têm maior dificuldade em aprovar, e a base de dados está

estruturada com linha para alunos e colunas para disciplinas, houve a necessidade, ainda no pré-processamento, de inverter a estrutura da base de dados. No *Rapid Miner* isso é possível com o uso do operador *Transpose* do módulo de pré-processamento. Assim, a base terá, após este processo, as linhas com disciplinas e as colunas com os alunos.

Para a mineração de dados, como adiantado anteriormente, escolheu-se o algoritmo *k*-Médias. Os parâmetros escolhidos para que o algoritmo segmentasse a base de dados foi $k=3$, pelas razões também discutidas anteriormente, e medida de distância Euclidiana.

Na próxima seção, os resultados obtidos são apresentados e, com isso, se apresenta também a avaliação e a interpretação dos experimentos, que é a última fase do processo de KDD (Figura 1).

4. Resultados

Os resultados apresentados a seguir mostram os grupos de disciplinas que, a partir do cálculo da média das notas dos alunos, propõe-se a classificação em difícil, regular e fácil. A partir do agrupamento, apresenta-se também como resultado as disciplinas segmentadas, permitindo uma análise quanto ao perfil de cada uma delas, ou seja, se as disciplinas são da área de programação, tecnológicas ou humanísticas. Estes resultados possibilitam, entre outras análises, a identificação de relações entre as disciplinas.

O resultado apresentado na Figura 3 relaciona a média final (eixo y) para cada aluno (eixo x). O desempenho do aluno em cada disciplina é visto no gráfico de dispersão, onde cada curva está rotulada por cores, de acordo com o grupo descoberto pelo algoritmo *k*-Médias.

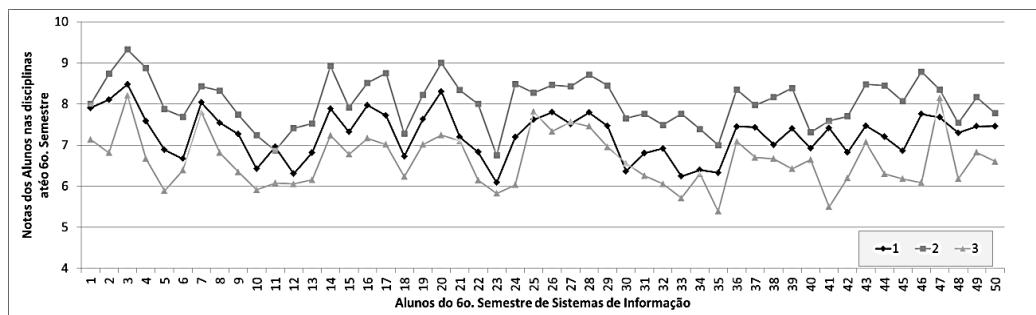


Figura 3. Série com as médias dos 50 alunos segmentadas em 3 grupos

A partir do resultado da Figura 3, deseja-se saber a média dos alunos em cada grupo de disciplina, junto com o desvio padrão. Esses resultados são apresentados na Figura 4, cujo resultado já permite classificar cada grupo de disciplinas, a partir da média. Ou seja, o grupo 3 é tido como aquele com disciplinas de menor média, $6,6 \pm 0,65$, e pode ser classificado como o grupo de disciplinas difíceis. O grupo 1, por outro lado, é o segundo de menor média, $7,2 \pm 0,57$, e pode ser classificado como disciplinas regulares. Por conseguinte, o grupo 2 tem disciplinas com média $8,0 \pm 0,58$, sendo classificada de disciplinas fáceis.

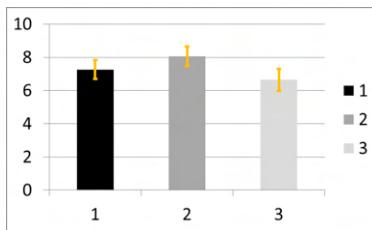


Figura 4. Histograma com os valores médios e respectivos desvios de cada grupo de disciplinas.

As disciplinas de cada grupo, agora já classificadas, são apresentadas na Tabela 2. Estas informações são importantes para saber a quantidade de disciplinas mapeada em cada um dos grupos e, também, para conhecer a relação entre elas, bem como o perfil das mesmas.

Avaliando as disciplinas da Tabela 2, é possível apresentar a porcentagem de disciplinas em cada grupo, Figura 4.

Tabela 2. Relação das disciplinas mapeadas em cada grupo

1	2	3
Éti. e Cida. I	Ing. Técn. I	Mat. para S.I. II
Mat. para SI I	Fun. S.I.	Arq. de Comp.
Amb. Oper.	Fun. de S.I. II	Mat. para S.I. III
Int. Prog.	Éti. e Cida. II	Est. de Dados II
Com. e Escr. Técn.	Ing. Técn. II	Ling. de Progr II
Est. de Dados I	Aná. de Proc. S.I.	Sis Oper
Ling. de Prog I	Téc. Prog. Apli. II	Mod. de Sist.
Tec. Web	Int. à Econ.	Sis. Dist.
Administração		Des. de BD
Eng. de Soft I		
Redes		
Pro. e Esta.		
Aná. de Sist. I		
Téc. Prog. Apli. I		
Int. à BD		
Pro. Inte. I		
Int. à Cont.		
Mat. Fina.		
Pes. Oper.		
MTC		
Eng. de Soft. II		
Direito		

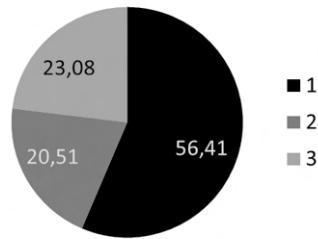


Figura 4. Distribuição das disciplinas mapeadas em cada grupo.

Com base em todas as informações descobertas, a partir do processo de agrupamento de dados, é importante que todos os resultados sejam summarizados, com o objetivo

principal de apresentar um conhecimento dos dados analisados. Estes resultados são apresentados na Tabela 3 e permitem um relacionamento das informações de classificação de cada grupo de disciplina, com os respectivos valores médios; um conhecimento sobre a porcentagem de disciplina no grupo; um conhecimento do perfil do grupo de disciplinas. Com esse último, consequentemente, é possível inferir o perfil de cada aluno no curso de Sistemas de Informação.

Dante os resultados apresentados, principalmente os que estão sumarizados na Tabela 3, é possível tirar alguns conhecimentos do perfil do curso, disciplina e alunos. Por exemplo:

- Matérias difíceis e de grande reprovação se encontram no grupo 3. Estas matérias representam 23,08% das disciplinas do curso e tem o perfil, basicamente, de programação. Com esse resultado se pode constatar a dificuldade dos alunos neste tipo de disciplina;
- A maior parte das disciplinas, 56,41%, se encontra no grupo 2, com média de $8,0 \pm 0,58$. Levando-se em conta que a média para aprovação na IES onde a pesquisa foi realizada é 6,0, pode-se afirmar que na maioria das disciplinas até o 6º. semestre, os alunos não têm dificuldade de aprovação;
- Ainda analisando as disciplinas do grupo 2, percebe-se que elas estão associadas, na maioria dos casos, com disciplinas humanísticas;
- O grupo 1 concentra disciplinas de Tecnologia e, também de Programação, e tem média final de $7,2 \pm 0,57$, acima da média para aprovação que é de 6,0;
- Resultados coerentes aparecem na classe regular, com 20,51% das disciplinas de programação e tecnologia;
- O aluno do curso de Sistemas de Informação da IES analisada, de modo razoável, tem dificuldades em disciplinas que envolvem programação.

Analizando as classes regular e fácil, juntas elas representam 76,92% das disciplinas. Em ambos os casos, o índice de aprovação é alto, lembrando que a média final no curso é de 6,0. Por outro lado, o nível de reprovação está abaixo dos 23,08%, o que pode ser considerado normal, pois trata-se de disciplinas de programação, o que é um problema nacionalmente conhecido em cursos de computação [Borges, 2000].

Tabela 3. Sumarização dos resultados descobertos pela análise de agrupamento

Classe	Grupo	Média	% disciplinas por grupo	Perfil do grupo de disciplinas
Diffícil	3	$6,6 \pm 0,65$	23,08	Programação
Regular	1	$7,2 \pm 0,57$	20,51	Programação e Tecnologia
Fácil	2	$8,0 \pm 0,58$	56,41	Humanísticas

5. Conclusão

Este trabalho apresentou o uso do k -Médias, uma técnica tradicional de agrupamento de dados, que faz parte da tarefa de mineração de dados, no processo de descoberta de conhecimento em bases de dados. Esse processo, também chamado de KDD, foi

apresentado de forma breve, porém, contextualizado no estudo de caso do artigo, agrupamento em notas de alunos do 6º Semestre de Sistemas de Informação. Por essa razão, o trabalho traz como particularidade no processo, o rotacionamento da base de dados, permitindo uma análise diferente da literatura que tradicionalmente analisa perfil de aluno. No entanto, neste trabalho analisamos o perfil das disciplinas. Adicionalmente, o trabalho apresenta uma ampla análise dos resultados que permite aos tomadores de decisão, os Coordenadores de Curso, um melhor conhecimento dos dados de notas e não apenas informações como média da turma, taxa de reproviação e etc manipuladas com SQL.

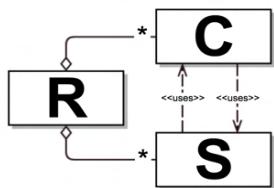
O resultado final apresentado no artigo se mostra coerente com a realidade deste tipo de curso em estudo. Ele pode ser considerado como exploratório, pois subsidia trabalhos futuros sobre fatores críticos de cursos e planos de ação para melhorar a qualidade de um curso superior ou fundamental. Ainda, é possível usar a metodologia apresentada neste trabalho como métrica para avaliar planos de ação aplicados com o objetivo de melhoramento de cursos e, assim, verificar impactos de mudanças no perfil dos alunos.

Estudos aprofundados no plano de ensino também devem ser considerados como trabalhos futuros para um melhor entendimento de resultados antagônicos como, por exemplo, classificação das disciplinas Estrutura de Dados I e Linguagem de Programação I em regulares e classificação das disciplinas Estrutura de Dados II e Linguagem de Programação II em difíceis.

Referências

- Borges, M. A. F. Avaliação de uma Metodologia Alternativa para a Aprendizagem de Programação. VIII Workshop de Educação em Computação – WEI 2000. Curitiba, PR, 2002
- Dias, M. M., Silva-Filho, L. A., Lino, A. D. P., Favero, E. L e Ramos, E. M. L. S. (2008) “Aplicação de Técnicas de Mineração de Dados no Processo de Aprendizagem na Educação a Distância”. In: SBIE - Simpósio Brasileiro de Informática na Educação, p. 105-114.
- Fayyad, U., Piatetsky-Shapiro, G., Smith, P (1996) “From Data Mining to KDD”. In: AI Magazine v. 17, n. 3, p. 37-54.
- Malvezzi, W. R., Mourão, A. B. e BRESSAN, G. (2010) Uma Ferramenta Baseada em Teoria Fuzzy para o Acompanhamento de Alunos Aplicado ao Modelo de Educação Presencial Mediado por Tecnologia” In: SBIE - Simpósio Brasileiro de Informática na Educação, v. Unico, p. 9.
- Marinho, T., Dermeval, D., Ferreira, R., Braz, L. M., Bittencourt, I. I., Costa, E.B. e Luna, H. P. (2009) “Um Framework para Mineração de Dados Educacionais Basedo em Serviços Semânticos”. In: WIE - Workshop de Informática na Escola, p. 2368-2373.
- Mierswa, I., Wurst, M., Klinkenberg R., Scholz, M. and Euler, E. (2006) “Yale: Rapid prototyping for complex data mining tasks” In Lyle Ungar, Mark Craven, Dimitrios Gunopulos, and Tina Eliassi-Rad, editors, KDD '06: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, p. 935-940.
- Pimentel, E. e Omar, N. (2006) “Descobrindo Conhecimentos em Dados de Avaliação da Aprendizagem com Técnicas de Mineração de Dados”. In: WIE - Workshop de Informática na Escola, p. 147-155.
- Romero, C., Ventura, S. e García, H. (2008) “Data mining in course management systems: Moodle case study and tutorial”. In: Computers & Education 51, pages 368-384.

- Romero, C., & Ventura, S. (2010). Educational data mining: a review of the state of the art. *Systems, Man, and Cybernetics, Part C: IEEE Transactions on Applications and Reviews*, 40(6), 601-618.
- Romero, C., & Ventura, S. (2007). Educational data mining: A survey from 1995 to 2005. *Expert Systems with Applications*, 33(1), 135-146.
- Silberschatz, A., Korth, H. F., & Sudarshan, S. (2006). Sistema de banco de dados. Campus.3a. edição.
- Witten, I.H., Frank, E. and Hall, M.A. (2011) Data Mining: Practical Machine Learning Tools and Techniques, Morgan Kaufmann, 3rd edition.



Uma Análise sobre o Uso de Metáforas em Ambientes Virtuais de Ensino

Beatriz de Almeida Pacheco¹, Ilana A. Souza-Concilio¹, Eliani Maria Kfouri²

¹Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Rua da Consolação, 930 – São Paulo – SP - Brasil

²Mboé Educação em Rede
Rua Carapuri, 26 – São Paulo – SP - Brasil

{bia.pacheco, iasouza}@mackenzie.br, e.kfouri@mboeeducacao.com.br

Abstract. This article aims to discuss the use of visual metaphors in the development of interfaces of education at distance systems. An important tool used to achieve the goals of usability is the use of such artifices that exploit users' prior knowledge and repertoire to facilitate the communication process to define computational interactions difficult to articulate. In LMSs the use of this resource is generalized, which may end by emphasizing similarities, omitting important differences between the model used as a reference and the system that is drawn from it. In this sense, this paper presents the findings about the use of metaphors obtained from tests carried out by two groups of users of virtual learning systems: students and teachers.

Resumo. Este artigo tem como objetivo discutir o uso de metáforas visuais no desenvolvimento de interfaces de sistemas de educação a distância. Uma ferramenta importante usada para atingir os objetivos de usabilidade é o uso de tais artifícios, que exploram o conhecimento prévio dos usuários e repertório para facilitar o processo de comunicação ao definir interações computacionais difíceis de articular. Em AVEAS seu uso é generalizado, o que pode acabar por enfatizar semelhanças, omitindo importantes diferenças entre o modelo usado como referência e o sistema que é desenhado a partir dele. Neste sentido, o presente trabalho apresenta as conclusões obtidas a partir de testes sobre o uso de metáforas realizados por dois grupos de usuários de sistemas virtuais de aprendizagem: estudantes e professores.

1. Introdução

Para aprimorar a educação formal a distância foram desenvolvidos sistemas chamados *Learning Management Systems*, ou Ambientes virtuais de Ensino e Aprendizagem (*LMS* – AVEAS em português), que são aplicações de softwares ou tecnologias baseadas em

Web utilizadas para planejar, implementar e avaliar um processo de aprendizagem específica. Normalmente, um sistema dessa natureza possui um instrutor (ou professor) que cria e distribui conteúdo, e comumente monitora a participação dos alunos e avalia seu desempenho. O AVEAS também pode proporcionar aos alunos a possibilidade de usar recursos interativos, como fóruns de discussão e chats. Em tais ambientes há cada vez um número maior de ferramentas disponíveis para promover um processo rico de ensino e aprendizagem.

De acordo com Levy (2003), novas mídias e seus suportes suscitam novos e diferentes tipos de conhecimento. Assim, por meio da experimentação em interfaces e dispositivos interativos, as pessoas passam a aprender de maneiras distintas, o que acaba por afastar as tecnologias e estratégias de ensino tradicional da nova realidade do aluno, construída a partir dessas novas relações.

Neste sentido, as interfaces devem ser projetadas visando as necessidades e expectativas dos utilizadores, permitindo-lhes direcionar sua atenção para os objetos com os quais trabalham diretamente, de uma forma rápida, eficaz, eficiente e satisfatória, o que significa que o projeto deve ser centrado no usuário [Roberts et. al, 1998].

Assim, com a finalidade de se aproximar do universo do usuário, o uso de metáforas visuais (ícones, gráficos, disposição dos elementos visuais na interface) pode explorar o conhecimento prévio dos usuários e seu repertório para facilitar o processo de comunicação, aproveitando o conhecimento já consolidado e transformando a aprendizagem mecânica em significativa [Ausubel, 1968]. Assim, portanto, permite a definição de interações computacionais geralmente difíceis de serem articuladas.

As metáforas permitem compreender e experimentar um tipo de coisa em termos de outra, recurso que é amplamente utilizado na vida cotidiana. Elas também podem ser usadas no projeto de interfaces digitais para alavancar o conhecimento prévio dos usuários e definir interações computacionais difíceis de articular [Preece, Rogers and Sharp, 2005].

No entanto, o uso inadequado da metáfora, bem como de outras figuras de linguagem, pode dificultar ou mesmo impedir algumas ações interativas. As metáforas enfatizam semelhanças entre duas coisas, mas também podem omitir diferenças [Lakoff and Johnson, 1980] [Blackwell, 2006]. Se o uso de figuras de expressão não é cuidadosamente feito, o usuário pode ser levado a crer que o sistema tem alguns atributos que certamente não possui.

Este artigo é parte de uma investigação anterior, que propôs uma análise das metáforas visuais utilizados pelo AVEA Moodle, com base na pesquisa e na classificação proposta por Lakoff e Johnson (1980). Sua intenção é analisar essas metáforas a partir de impressões do usuário e de sua percepção. Nesse sentido foram analisados professores e alunos. Eles foram divididos em dois grupos, aqueles que já estavam familiarizados com o Moodle, e aqueles que nunca haviam interagido com o LMS analisado. Como metodologia de ensaio, utilizou-se a proposta de Nielsen (2000), com um número limitado de usuários.

F2. As metáforas: características e classificações

A partir da publicação de “Metaphors we live by”, por Lakoff e Jonhson (1980), diversos investigadores passaram a defender a ideia de que metaforizar processos é

característica inerente ao ser humano, fenômeno constituinte da cognição e linguagem humana. Para eles, a linguagem é inherentemente metafórica e presente desde as linguagens mais poéticas às mais rigorosas, como a linguagem científica.

O termo metáfora usado no design de interface é um pouco diferente do mesmo termo usado na literatura. Na literatura significa "uma comparação implícita entre duas coisas ao contrário de natureza que ainda têm algo em comum" [Corbett and Connors, 1999]. A importância da metáfora está em fazer um novo sistema se parecer e agir como um sistema já conhecido: metáforas de interface dão ao usuário um modelo a ser seguido, sem que haja necessidade que ele crie o seu.

No entanto, mesmo neste ambiente, deve-se atentar ao fato que o significado almejado pelo designer por meio de uma construção metafórica pode não ser entendida e estabelecida pelo usuário, uma vez que os elementos envolvidos na origem e destino decorrem de experiências pessoais. Contudo, este aspecto depende do tipo da metáfora produzida. As metáforas mais convencionais costumam aproximar de forma mais natural os processos de produção e compreensão, o que acaba por tornar menos importante o contexto e situação na construção de sentido [Gibbs, 1994; 2002].

Lakoff e Johnson (1980) explicam que as metáforas estão infiltradas na vida cotidiana, não somente na linguagem, mas no pensamento e na ação. Isso significa que os conceitos que estruturam os pensamentos orientam também o modo como as pessoas percebem, se comportam e se relacionam no mundo: de acordo com sua experiência física e cultural.

Existem várias classificações para metáforas. Por exemplo, elas podem ser classificadas de acordo com os termos linguísticos, de acordo com as relações envolvidas na associação, no que diz respeito ao tempo de sua adoção, entre outros.

Entre as classificações estudadas, algumas foram identificadas como apropriadas para Web. Destas, duas se destacam: uma é classificar metáforas de acordo com o tipo de relação entre os dois elementos envolvidos na associação e a outra é de acordo com seu tempo de existência [Lakoff and Johnson, 1980] [McLaren, 2000].

1. A classificação como função do relacionamento: este tipo de classificação envolve metáforas que relacionam uma coisa a outra. As relações envolvidas podem levar a:

- A. Metáforas estruturais: são usados para comparar um conceito a conceitos cotidianos [McLaren, 2000]. Eles caracterizam o conceito de estrutura em comparação com a estrutura de um outro processo [Lakoff and Johnson, 1980].
- B. Metáforas Orientacionais: transmitem o conceito de orientação espacial (para cima, para baixo), ou seja, um conceito explicado em termos de espaço. Eles organizam todo um sistema de conceitos de uma forma para se tornar possível relacionar um conceito para uma relação espacial [Lakoff and Johnson, 1980].
- C. Metáforas ontológicas: relacionam conceitos em termos de categorias básicas da existência como objetos ou como substâncias. A compreensão das experiências em termos de objetos ou substâncias permite selecionar partes da experiência e tratá-las como entidades discretas ou substâncias de um tipo de uniforme [Lakoff and Johnson, 1980].

2. Classificação em função da Existência: relaciona-se com a forma como as pessoas recebem as metáforas relativas uma coisa a outra: envolve uma relação já conhecido e familiar ou traz uma nova concepção de relacionamento que mostra um novo conceito.

- A. Metáforas convencionais: são aqueles já utilizados intuitivamente pelas pessoas. No ambiente Web, ele pode ser considerado tradicional, que já existia como interfaces gráficas digitais antes da popularização da Internet.
- B. Novas metáforas: são aqueles ainda não utilizados intuitivamente pelas pessoas. Neste caso, a estrutura da metáfora deve ser previamente estabelecida [McLaren, 2000].

4. Usabilidade: Conceitos e Testes

Atualmente, com o surgimento dos games, smartphones e outros dispositivos, usuários passaram a esperar algo mais agradável e intuitivo em interfaces, o que os torna mais críticos em relação aos produtos de operação complicada [Farias, 2002].

Usabilidade visa o desenvolvimento de interfaces que permitem a interação fácil, agradável, eficaz e eficiente. Deve permitir a criação de interfaces transparentes de modo a não dificultar o processo, permitindo o controle total do ambiente do usuário sem recorrer a um obstáculo durante a interação [Nielsen and Loranger, 2003] [Nielsen, 1993].

A forma mais comum de avaliar a capacidade de utilização de um sistema é a partir do acompanhamento da interação do usuário. Isto pode ser feito em um laboratório com uma quantidade representativa de utilizadores para os quais o sistema foi desenvolvido ou no ambiente de trabalho, onde o sistema vai ser implantado.

De acordo com Nielsen (1993) é possível, a partir de testes realizados com apenas cinco usuários, identificar a maioria dos problemas de usabilidade de um sistema. De acordo com o autor, quando o primeiro usuário é testado, cerca de um terço dos problemas de projeto e de usabilidade já podem ser resolvidos. A partir do segundo usuário testado, muitos dos problemas apontados pelo primeiro são percebidos novamente, e alguns outros são identificados. Esta série novas percepções vai diminuindo rapidamente, e, a partir do sexto usuário dificilmente alguma coisa nova e importante é detectada.

Nielsen (2000), afirma que com 5 usuários sendo testados, é possível identificar cerca de 85% dos problemas, e “distribuir seu orçamento para testes com usuários em vários pequenos testes em vez de despender tudo em um único estudo”. Portanto, não há nenhuma necessidade real de se fazer testes com muitos usuários, após o quinto usuário, “você está desperdiçando seu tempo observando os mesmos resultados repetidamente, mas não está aprendendo muita coisa nova” [Nielsen, 2000].

5. Metáforas em AVEAs: O Caso Moodle

Em ambientes virtuais de ensino e aprendizagem o uso de metáforas também é generalizado. Nesses espaços, a principal função desses elementos é de facilitar a navegação do aluno e do professor, possibilitando o acesso, interação e edição de conteúdo de forma interativa e imediata.

Para analisar o uso de metáforas em tais ambientes, esta pesquisa considerou o AVEA Moodle, plataforma desenvolvida colaborativamente e de distribuição gratuita. Devido

a sua natureza, muitos desenvolvedores ao redor do mundo criam seus próprios temas (interfaces gráficas), que tendem a usar elementos visuais de bibliotecas existentes ou a desenvolver sua própria família de elementos gráficos. De um jeito ou de outro, muitos deles começam a partir de associações comumente vistas nas interfaces do sistema operacional Linux, que é projetado de forma semelhante ao LMS em questão [Pacheco and Kfouri, 2012].

Para analisar os elementos de imagens metafóricas, foram analisados os ícones padrão da ferramenta e aqueles usados no skin da interface utilizada pela Instituição de Ensino Superior. Ícones pertencentes a todas as categorias apresentadas por Moknern (1997) e Lakoff e Johnson (1980) foram encontrados.

5.1. Análise de metáforas visuais de acordo com a percepção do usuário

Para a coleta de dados precisos, os usuários foram divididos em dois grupos: os que ainda não tiveram contato com a plataforma (01) e os que já tiveram contato com a plataforma (02). Além disso, eles foram também divididos em: alunos (A) e professores (P). Portanto, nas análise aparecerão notações do tipo: P01, P02 ou A01 e A02. A eficiência das metáforas visuais foi testada a partir de um questionário on-line respondido por eles.

Os grupos de estudantes são os que interessam mais a pesquisa pois, como apontado no presente estudo, uma interface de interação que proporciona comandos intuitivos e transparentes proporciona a possibilidade de aumento de gasto de energia do aluno no processo de ensino e aprendizagem (conteúdo a ser aprendido), objetivo primeiro de sua interação.

Este questionário tem quatro grupos de questões: perfil do usuário, perguntas abertas, em que o usuário deve associar as imagens apresentadas a um conceito (área de ação / tarefa / aplicação), questões de múltipla escolha em que os usuários devem associar a imagem apresentada um dos conceitos fornecidos, e associações livres em que o usuário deve associar uma imagem (em sua cabeça) aos conceitos apresentados.

Quinze (15) estudantes e cinco (5) professores de cada grupo foram testados com base na metodologia de Nielsen (2000).

5.2. Análise dos resultados

Grupo de Alunos:

O grupo A01 é composto por 15 estudantes universitários que, apesar de usar um LMS na instituição em que estudam, este não é Moodle. Dessa forma eles não estão familiarizados com as metáforas visuais apresentadas. Este grupo apresenta um equilíbrio de gênero (8 mulheres e 7 homens) e de idade (87% entre 18 e 25 anos).

Já o grupo A02 é formado por estudantes predominantemente jovens (67% tem entre 18 e 25 anos) que utilizam o Moodle diariamente. Vale a pena destacar o pequeno número de mulheres pesquisadas nesse grupo pelo fato destes pertencerem à cursos ligados à tecnologia (apenas uma).

A seguir são destacadas algumas respostas emblemáticas da pesquisa. Os primeiros exemplos foram colhidos a partir do grupo de questões abertas.

Uma das imagens mostradas aos usuários foi a que representava “meus arquivos privados” (Figura 01a). Embora não houvessem suposto corretamente o nome da área no AVEA, 73% da primeira amostra (grupo A01) fez a associação adequada. Já no Grupo A02, formado por usuários do sistema, surpreendentemente nenhum deles foi capaz de associar o ícone que representa a sua área de trabalho cotidiano (“meus arquivos privados”), mas 86% fizeram uma associação correta com a ideia do que ele representava.



Figura 01. Ícones: (a) “Meus arquivos privados”; (b) Calendário

A imagem representada na Figura 01b, Calendário, por sua vez, refere-se a uma representação comum em interfaces digitais. Neste caso, 100% das associações feitas pelo grupo A01 foram próximas da função do ícone, e, dentre elas, 66% usaram exatamente a denominação usada no AVEA.

Já no grupo A02, todos os alunos fizeram associações apropriadas e 93% fizeram exatamente a associação proposta pelo Moodle da Universidade em que estudam.

Uma outra associação que mostrou resultados interessantes foi a que dizia respeito ao Glossário do Moodle. Uma metáfora que expressa uma área típica nos ambientes virtuais de ensino e aprendizagem e que costuma estar presente na maioria das interfaces, foi apontada por apenas um dos alunos analisados no grupo A01, enquanto apesar de usarem a interface diariamente, apenas dois alunos do segundo grupo fizeram a associação esperada.

Outro resultado semelhante ocorreu quando foi analisado o ícone que representava “meus cursos” no AVEA (Figura 02). Nenhum dos alunos do grupo A01 foram capazes de fazer associações apropriadas. Em contraste, 53% fez uma mesma associação errada, o que prejudica a compreensão da interface. Já no grupo A02, apenas um dos entrevistados foi capaz de fazer uma associação apropriada.



Figura 02. Meus cursos

No grupo de múltipla escolha pode-se destacar o resultado para o ícone “editar” (Figura 03a). Do primeiro grupo de usuários, 66% dos fez associação correta, enquanto no segundo grupo esse número caiu para apenas 40%, apesar do fato desses alunos lidarem diariamente com a metáfora.

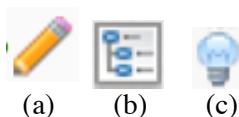


Figura 03. Ícones para (a) “editar”; (b) “lição” e (c) “área ativa”

O segundo elemento refere-se aos trabalhos apresentados, lições (Figura 03b). Note que o nome e a divisão das atividades na plataforma, na versão em Português, muitas vezes faz com que haja alguns mal-entendidos, pois as palavras tarefas e lição costumam ser usadas como sinônimos. Assim, pela familiaridade com a plataforma, o número de associações assertivas aumenta significativamente, 40% no grupo A02 contra 6% no grupo A01.

Sobre o ícone que representa “área ativa” (Figura 03c), para os alunos que não conhecem a plataforma o significado associado é o de ideia (80%). No grupo A02, apesar do contato próximo, nenhum aluno indicou “área ativa” enquanto 66% também fez associação à ideia, como no primeiro grupo.

Finalmente sobre as questões associativas, quando a palavra solicitada foi “mensagem”, 73% dos entrevistados do primeiro grupo associaram a palavra a um envelope de carta e 20% a um balão de fala. Já no grupo A02, 100% dos entrevistados associaram a palavra com um envelope de carta, como no Moodle de sua Universidade.

Sobre o tópico “Edição”, 73% dos entrevistados do primeiro grupo fez a associação com um lápis, assim como os usuários do sistema, que fizeram a associação numa porcentagem semelhante (70%).

Já sobre “configurações”, destaca-se que 66% dos entrevistados associou a palavra com engrenagens no grupo A01 enquanto cerca de 80% do segundo grupo fez a mesma associação.

Grupo de Professores:

Foram testados dois grupos de professores com características semelhantes às dos alunos testados: não conhecedores/usuários do sistema (P01) e conhecedores/usuários do sistema (P02).

O grupo P01 foi composto por 05 professores universitários que usam um LMS na instituição em que trabalham, mas não é o Moodle. Assim, eles não estão acostumados com as metáforas visuais apresentadas. O grupo P02 consiste de professores da Instituição de Ensino Superior, familiares com a ferramenta.

Ambos os grupos são compostos por quatro homens e uma mulher; 70% dos entrevistados têm mais de 41 anos de idade, 20% têm entre 36 e 40 anos e 10% entre 31 e 35 anos.

Os mesmos testes realizados com os alunos também foram aplicados aos professores. Algumas respostas emblemáticas da pesquisa são destacadas a seguir. Os primeiros exemplos foram coletados do grupo de questões abertas.

Em relação à imagem que representa "meus arquivos privados" (Figura 01a), o primeiro grupo de usuários (P01), ao visualizar este ícone, fez uma associação com arquivo ou diretório; apenas um professor destacou a pasta pessoal. No grupo P02, formado por usuários do sistema, apenas um professor não fez a associação corretamente.

Já sobre a imagem que representa o calendário (Figura 01b), 80% das associações produzidas por ambos os grupos estavam corretas. Entre os professores que utilizam o

sistema e os demais testados que fizeram a associação correta, todos usaram exatamente a mesma nomenclatura usada pelo Moodle.

A associação que também mostrou resultados interessantes foi sobre o Glossário do Moodle. Uma metáfora que se refere a uma área típica de ambientes virtuais de ensino e aprendizagem e que é geralmente apresentada na maioria das interfaces, não foi nomeada por qualquer professor como era esperado.

Quanto ao ícone que representa "meus cursos" (Figura 02) no AVEA analisado, nenhum dos professores de ambos os grupos foi capaz de fazer a associação desejada pelos desenvolvedores.

É possível destacar o resultado para o ícone "editar" no grupo de múltiplas escolhas (Figura 03a). No primeiro grupo de usuários (P01), 80% fez a associação correta, enquanto que no segundo grupo (P02) este número desceu para apenas 60%, apesar do fato de estes professores lidarem diariamente com a metáfora.

No caso do elemento referente aos trabalhos apresentados em aulas, lições (Figura 03b), verificou-se que em ambos os grupos 40 % dos membros fez a associação correta.

Sobre o ícone que representa "área ativa" (Figura 03c), para usuários que não conhecem a plataforma, o significado associado foi o de ideia (100%). Já grupo P02, embora existisse o contato diário com a plataforma, apenas um professor indicou "área ativa", enquanto o restante relacionou a imagem com o conceito de ideia, como no primeiro grupo.

Finalmente, sobre as questões associativas, quando “mensagem” era a palavra solicitada, 100% dos entrevistados associaram a palavra ao envelope.

O lápis, por sua vez, foi a imagem indicada por quase todos os entrevistados quando perguntados sobre a função de edição. Apenas um professor, que não estava familiarizado com a interface, optou por um conjunto de ferramentas.

Sobre "configuração", destaca-se que todos os participantes do grupo P02 fez a associação desejada com engrenagens, enquanto as respostas do primeiro grupo (P01) foram variadas: sistemas, engrenagens de controle e pessoa.

Percebe-se, então, neste último grupo de questões, uma uniformidade maior nas respostas, o que indica a aproximação de significados das metáforas cujas ideias estão mais presentes nos Sistemas Digitais de um modo geral, sejam eles sistemas operacionais, interfaces web ou AVEAs.

Sobre alunos e professores: discussão

Como as metáforas, por muitas vezes, são utilizadas de maneira excessiva no desenvolvimento de sistemas interativos, alguns autores, como Donald Norman (1999) são céticos com relação ao seu uso. Para ele, o uso de metáfora é errado por definição uma vez que utilizá-las significa usar um objeto não necessariamente ligado ao propósito do sistema para que se estabeleça a relação. O autor defende a necessidade de se desenvolver um novo modelo conceitual compreensível que descreva os elementos constituintes da interface pelo que eles fazem e são. Segundo ele, a partir desse novo modelo, o usuário poderá aprender a interagir com a interface [Norman, 1999].

Nielsen e Loranger (2003), por sua vez, acreditam que metáforas podem ser usadas de forma cautelosa. Apesar dos autores acreditarem que muitas vezes é melhor desenvolver

um novo modelo conceitual, eles afirmam que seu uso traz benefícios, como o de facilitar o aprendizado dos usuários que poderão então usar um sistema com base em uma referência já familiar.

A partir da presente pesquisa teórica e dos resultados práticos obtidos por meio das análises dos testes realizados por professores e alunos, familiarizados ou não com a interface pesquisada, tende-se a concordar com a posição de Jakob Nielsen, que prega o uso cauteloso de tais associações.

Apesar das constatações de Lakoff e Johnson (1980) de que as metáforas estão infiltradas na vida cotidiana das pessoas, não somente em sua linguagem, mas pensamento e ação, quando se está diante de um sistema interativo tais associações podem variar muito conforme o repertório do usuário, e elementos projetados inicialmente para incrementar interações, podem acabar por comprometê-las. Ou seja, como já foi dito anteriormente, a experiência física e cultural, estão presentes e influenciam o modo como as pessoas percebem, se comportam e se relacionam no mundo.

Assim, deve-se atentar ao fato que o significado almejado pelo designer por meio de uma construção metafórica pode não ser entendida e estabelecida pelo usuário, uma vez que os elementos envolvidos na origem e destino decorrem de experiências pessoais [Gibbs, 1994; 2002].

A avaliação de metáforas com estudantes e professores mostrou que a familiaridade com o sistema realmente resolve alguns problemas associativos enquanto há o aprendizado de elementos visuais metafóricos. No entanto, esses elementos, se analisados fora do contexto de associação, podem resultar em associações truncadas ou incipientes. Nestes casos, percebe-se uma elevada sobrecarga cognitiva, o que sugere a utilização de texto complementar às metáforas ou ainda a substituição completa de tal recurso.

Assim, os resultados apresentados na presente pesquisa apontam para muitas dessas associações no ambiente Moodle serem equivocadas e não consoantes às experiências anteriores dos usuários analisados.

Ao se testar os usuários e se considerar suas experiências é possível preencher a lacuna existente em relação às motivações e necessidades das pessoas no processo de interação com sistemas e se propor metáforas que, de fato, possam auxiliar o processo interativo.

6. Considerações Finais

A análise revelou que, embora as metáforas possam fazer o usuário se sentir mais confortável em lidar com ideias e conceitos familiares, eles não determinam um objeto a se comportar exatamente como o outro. Durante a interação, o usuário terá que melhorar o padrão conceitual, porque o mais perto que eles podem ser o mundo da informática é diferente do real, por isso concluiu-se que as metáforas podem ser usadas, mas com cuidado e cautela.

Em termos cognitivos, os procedimentos analógicos dependem de conceitos mais concretos e mais perto da experiência dos usuários. Portanto, eles podem estender sua compreensão para níveis mais complexos e abstratos de conhecimento e apreensão da realidade. Este procedimento é altamente produtivo na ampliação e renovação do vocabulário de uma língua.

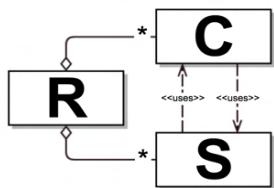
Embora tradicionalmente visto como um processo eminentemente semântico, ele realmente opera com regras pragmáticas. Se entendida apenas no nível semântico, a analogia metafórica pode não ser totalmente decodificada pelo receptor. As inferências não são dedutíveis de significados pragmáticos de regras lógicas, mas de regras de conversação, que são decorrentes das relações contextuais.

Como extensão desta pesquisa, pretende-se realizar outros testes em Ambientes Virtuais de Ensino e Aprendizagem com a finalidade de identificar um conjunto de metáforas que apresentem resultados ótimos em relação às relações que estabelecem com o que pretender ser ou fazer.

Referências Bibliográficas

- Ausubel, D.P. (1968). Educational psychology: a cognitive view. New York, Holt, Rinehart and Winston.
- Blackwell, A. F., 2006. The reification of metaphor as a design tool- ACM Transactions on Computer-Human Interaction (TOCHI) Vol.13, N.4, pg: 490–530.
- Corbett, Edward P. J., Connors, Roberts J., 1999. Classical Rhetoric for the Modern Student. New York, NY :Oxford University Press.
- Farias, Priscila (2002). Sign design, ou o design dos signos: a construção de diagramas dinâmicos para as classes de signos de C. S. Peirce. Tese de doutorado não publicada, Programa de Estudos Pós-Graduados em Comunicação e Semiótica, Pontifícia Universidade Católica de São Paulo.
- Gibbs, R. W., Jr. (2002).A new look at literal meaning in understanding what is said and implicated .Journal of Pragmatics, v.34, p.457-486.
- Gibbs, R. W., Jr.. (1994). The poetics of mind figurative thought language and understanding. Cambridge: Cambridge University Press.
- Lakoff, G.and Johnson, M., 1980. Metaphors we Live By. Chigago, IL:The University of Chicago Press.
- Levy, Pierre, 2003. A inteligência coletiva: por uma antropologia do ciberespaço. 4.ed. São Paulo, SP: Loyola.
- McLaren, Ian (2000). “Some pictorial symbol systems for public places”. In:Masoud Yazdani and Philip Barker (eds.) Iconic communication , pp. 42-50.Bristol: Intellect.
- Mokn kern, K., 1997. Visual Interaction Design: Beyond the Interface Metaphor – SIG- CHI Vol 29, n.2. Disponível em: <http://old.sigchi.org/bulletin/1997.2/vid.html#HDR3> Acesso em: 02/02/2012.
- Nielsen, J. (1993). Usability Engineering. San Francisco, CA: Morgan Kaufmann.
- Nielsen, J. and Loranger,H.,(2003). Prioritizing Web Usability. 1 Ed. Berkeley, CA: New Riders Press.
- Nielsen, J., 2000. Why You Only Need to Test with 5 Users. Disponível em <http://www.useit.com/alertbox/20000319.html>. Acesso em 14/03/2012.

- Norman, D.A. (1999). *The Invisible Computer: why good products can fail, the personal computer is so complex, and information appliances are the solution.* Massachusets-The MIT Press.
- Pacheco, B. And Kfouri, E., (2012). Use of virtual metaphors in virtual environments: classification and uses. Proceedings of The International Conference on Innovations in Learning and Technology: Asia-Pacific Perspectives. University of Victoria, CA.
- Preece, J., Rogers, Y. and Sharp, H., 2005. *Design de Interação, além da Interação Homem- Computador*. São Paulo, SP: Bookman.
- Roberts, D., Berry, D., Isensee, S. and Mullaly J., 1998. *Designing for the user with OVID: Bridging User Interface Design and Software Engineering.* MacMillan Technical Publishing - Software Engineering Series.



Fortalecimento do Esquema de Criptografia por Curvas Elípticas via Rotações Tridimensionais

Daniel Lackeski Suigh Carlos, Luciano Silva

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Caixa Postal 930 – 01.302-907 – São Paulo – SP – Brasil

danscarlos@gmail.com, luciano.silva@mackenzie.br

Abstract. *The elliptic curve cryptography is a feasible alternative to the traditional RSA method. It uses the difficulty of solving the discrete logarithm problem in an algebraic field defined by an elliptic curve. Within this context, the development of techniques to strength this cryptography method has both academic and commercial interest. This work presents the elliptic curve cryptography, with its arithmetic and vulnerabilities. The objective is to investigate a way of using rotations about the x axis to improve this cryptographic scheme. A new cryptography method was elaborated, which takes advantage of 3D rotations to increase the cryptoanalysis difficulty. Tests were conducted to indicate that the proposed method is capable of encrypting and decrypting messages.*

Resumo. *A criptografia por curvas elípticas representa uma alternativa muito interessante ao tradicional método RSA. Ela utiliza a dificuldade de resolver o problema do logaritmo discreto em um corpo algébrico definido por uma curva elíptica. Dentro deste contexto, o desenvolvimento de técnicas que fortaleçam este criptográfico possui não só interesse acadêmico quanto comercial. Este trabalho apresenta a criptografia com curvas elípticas, juntamente com sua aritmética e suas vulnerabilidades. A proposta é investigar uma forma de utilizar rotações em torno do eixo x para fortalecer esse esquema de criptografia. Para isso, foi elaborado um novo método de criptografia com curvas elípticas, que utiliza essas rotações para aumentar a dificuldade de se fazer a criptoanálise. No final, testes realizados indicam que o método proposto foi capaz de codificar e decodificar mensagens.*

1. Introdução

A criptografia com curvas elípticas foi descoberta em 1985 por Neal Koblitz e Victor Miller, e seu funcionamento é baseado em outros esquemas de criptografia com chave pública. Esses é um tipo de criptografia assimétrico, ou seja, o método

usado para codificar uma mensagem não pode ser invertido para decodificá-la, garantindo, dessa forma, que os detalhes do funcionamento de tal método possam ser tornados públicos sem que sua segurança seja comprometida. No caso da criptografia com curvas elípticas, a assimetria está na forma que as operações entre os pontos da curva são definidas. Quando um determinado ponto é somado a ele mesmo n vezes, é difícil encontrar n a partir do resultado, pois não existe uma operação de divisão para reverter esse procedimento.

Esse tipo de criptografia apresenta uma grande vantagem quando comparado aos outros esquemas criptográficos de chave pública, pois ele é baseado no problema do logaritmo discreto sobre curvas elípticas. Como não existe uma forma de ataque em tempo sub-exponencial para esse problema, é possível utilizar chaves menores sem aumentar a sua vulnerabilidade. Por exemplo, uma chave RSA de 1024 bits equivale a uma chave de uma curva elíptica de 160 bits em termos de segurança [Wong, 2009].

O objetivo desse trabalho é de fortalecer o esquema de criptografia com curvas elípticas. Para isso, rotações ao redor do eixo x serão aplicadas aos pontos da curva, para que, dessa forma, seja criada uma ambiguidade quanto à origem de cada ponto que precisar ser tornado público, e dificultando a operação dos métodos de criptoanálise.

Conforme avanços tecnológicos permitem que os computadores fiquem mais rápidos, as chaves dos métodos de criptografia ficam mais vulneráveis e, por isso, devem ter sua quantidade de bits aumentada. Porém, chaves maiores possuem uma série de desvantagens, como a necessidade de mais espaço e o fato de apresentarem uma dificuldade maior de serem calculadas. Por isso, se faz necessário que métodos mais eficientes e robustos de criptografia sejam pesquisados. Neste cenário, o presente trabalho pretende contribuir para que a criptografia com curvas elípticas, que já é mais eficiente que outros métodos, possa ser fortalecida sem a necessidade de utilizar chaves maiores. Dessa forma, o surgimento de computadores mais avançados terá um impacto reduzido na segurança desse tipo de criptografia.

2. Criptografia com Curvas Elípticas

2.1. Corpos Finitos F_p

Um corpo finito é um conjunto munido de duas operações binárias: adição e multiplicação. Os corpos finitos primos F_p possuem os seguintes elementos: $\{0, 1, \dots, p-1\}$.

A adição entre dois elementos a e b pertencentes a F_p é dada por $a + b = r \pmod{p}$. Para realizar a subtração de a por b , basta realizar a soma de a com o negativo de b , que é a solução da equação $b + x = 0 \pmod{p}$.

A multiplicação entre dois elementos a e b pertencentes a F_p é dada por $ab = s \pmod{p}$. Para realizar a divisão de a por b , basta multiplicar a pelo inverso de b , que é a solução da equação $bx = 1 \pmod{p}$.

2.2. Curvas elípticas sobre corpos finitos do tipo F_p

Uma curva elíptica E sobre o corpo F_p é definida pela equação: $y^2 = x^3 + ax + b$. O conjunto $E(F_p)$ é composto por todos os pontos $(x, y) \in F_p$ que satisfazem à essa equação junto com o ponto no infinito O .

Para que a adição em $E(F_p)$ possa ser definida, é necessária a definição de um novo símbolo: Θ .

Definição 1: Sejam (x_1, y_1) e $(x_2, y_2) \in E(F_p)$, define-se Θ da seguinte forma:

- Se $(x_1, y_1) = (x_2, y_2)$, então $\Theta = (3x^2 + a) / 2y$
- Se $(x_1, y_1) \neq (x_2, y_2)$, então $\Theta = (y_2 - y_1) / (x_2 - x_1)$.

Com base em Θ , define-se a adição de pontos em $E(F_p)$:

Definição 2: A adição de dois pontos em $E(F_p)$ é dada da seguinte forma:

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, onde:

- $x_3 = \Theta^2 - x_1 - x_2$
- $y_3 = \Theta(x_1 - x_3) - y_1$.

O conjunto $E(F_p)$ com a operação de adição forma um grupo e sua identidade é ponto O . O negativo do ponto (x, y) é $(x, -y)$, pois $(x, y) + (x, -y) = O$.

Cada ponto na curva possui uma ordem, isto é, o tamanho do ciclo gerado quando ele é somado a si próprio n vezes. De acordo com Wong (2009), a ordem de um ponto é definida formalmente da seguinte forma:

Definição3: Dado o ponto $P \in E(F_p)$, a ordem n de P é o menor inteiro que resolve: $nP = O$, onde O é o ponto no infinito.

2.3. Métodos para curvas elípticas

Agora, será definido um sistema criptográfico análogo ao sistema proposto por ElGamal, baseado no Problema do Logaritmo Discreto [ElGamal, 1985].

Antes de criptografar uma mensagem, é necessário decidir qual tipo de corpo será utilizado, os parâmetros da curva elíptica E , e um ponto base $P \in E$, que serão tornados públicos. Cada usuário desse sistema deve, então, escolher um número n , que será sua chave secreta, e calcular nP , que será sua chave pública.

Assumindo que Alice queira mandar a mensagem m para Bob, ela deverá primeiro representar m através de um ponto P_m na curva E . Alice conhece a chave pública de Bob n_bP , então para criptografar P_m ela escolhe um inteiro k e envia para Bob o seguinte par de pontos: $(C_1, C_2) = (kP, P_m + k(n_bP))$. Para decifrar o texto, Bob calcula $C_2 - n_bC_1 = (P_m + k(n_bP)) - n_b(kP) = P_m$.

Existe, também, uma outra forma de criptografar dados para curvas elípticas, o método Menezes-Vanstone (Menezes e Vanstone, 1993). Nesse método, ao invés de ser enviado um par de pontos como no método anterior, é enviado o

conjunto com um ponto e dois números $Y = (y_0, y_1, y_2)$. A seguir, seu funcionamento será detalhado.

Primeiramente, define-se o corpo finito que será utilizado e os parâmetros da curva elíptica E , bem como um número aleatório k pertencente ao corpo finito escolhido. A chave secreta é s , e a chave pública é o par de pontos (Q, P) , onde $P \in E$ e $Q = sP$. Sendo $X = (x_1, x_2) \in E$ a mensagem a ser criptografada, calcula-se componentes de Y que serão transmitidos em da seguinte forma:

- $y_0 = kP$
- $y_1 = c_1 x_1$
- $y_2 = c_2 x_2$

$$\text{onde } (c_1, c_2) = kQ.$$

Ao receber $Y = (y_0, y_1, y_2)$, a mensagem original $X = (x_1, x_2)$ é recuperada da seguinte forma:

- $x_1 = y_1(c_1)^{-1}$
- $x_2 = y_2(c_2)^{-1}$

$$\text{onde } (c_1, c_2) = s^* y_0.$$

3. Métodos de Criptoanálise em Curvas Elípticas

3.1. Método Pollard rho

O método Pollard rho [Pollard, 1978] é usado para resolver o problema do logaritmo discreto. O algoritmo abaixo mostra como ele pode ser adaptado para resolver o problema do logaritmo discreto sobre curvas elípticas, conforme Hankerson, Menezes e Vanestone (2004):

Entrada: Curva elíptica $E(F_p)$, ponto base P de ordem n , chave pública Q .

Saída: Chave privada k .

1. Selecionar a quantidade L de subgrupos para dividir os pontos de $E(F_p)$.
2. Criar uma função de partição H para dividir os pontos de $E(F_p)$ entre os L subgrupos.
3. Repetir para j de 1 até L
 - 3.1. Selecionar aleatoriamente $a_j, b_j \in [0, n-1]$.
 - 3.2. Computar $R_j = a_j * P + b_j * Q$.
 4. Selecionar aleatoriamente $c', d' \in [0, n-1]$ e computar $X' = c'^* P + d'^* Q$.
 5. Atribuir os valores: $X'' = X'$, $c'' = c'$, $d'' = d'$.
 6. Repetir
 - 6.1. Computar $j = H(X')$.
Atribuir valores: $X' = X' + R_j$, $c' = c' + a_j \bmod n$, $d' = d' + b_j \bmod n$.
 - 6.2. Para i de 1 até 2:
Computar $j = H(X')$.
Atribuir valores: $X'' = X'' + R_j$, $c'' = c'' + a_j \bmod n$, $d'' = d'' + b_j \bmod n$.
Até que $X' = X''$.
 7. Se $d' = d''$ retornar "falha".

3.2. Método Pohlig-Hellman

O método Pohlig-Hellman foi proposto como uma forma de resolver o problema do logaritmo discreto sobre F_p , com complexidade $O(\log^2 p)$ se $p-1$ possuir fatores

primos pequenos [Pohlig, Hellman, 1978]. O algoritmo exibido na próxima página, baseado em Barker (2008), mostra como ele pode ser usado para resolver o problema do logaritmo discreto sobre curvas elípticas.

Entrada: Curva elíptica $E(F_p)$, ponto base P de ordem n , chave pública Q .

Saída: Chave privada k .

1. Fatorizar n em seus r fatores: $l_1^{e1}, l_2^{e2}, l_3^{e3} \dots l_r^{er}$.
2. Repetir para j de 1 até r
 - 2.1. Definir as constantes $P_0 = n/l_j * P$, $Q_0 = n/l_j * Q$ e $k_j = 0$.
 - 2.2. Criar uma lista $T = \{a * P_0 \mid 0 \leq a \leq l_j - 1\}$.
 - 2.3. Repetir para i de 0 até $e_j - 1$
 - 2.3.1. Se $i > 0$, $Q_i = n/l_j^{i+1} * (Q_{i-1} - k_{i-1} * l^{i+1} * P)$.
 - 2.3.2. Encontrar na lista T o elemento a_i que satisfaça: $Q_i = a_i P_0$.
 - 2.3.3. Calcular $k_j = k_j + a_i * l^i$.
 3. Resolver o sistema de congruências $k = k_1 \text{ mod } l_1^{e1}$ (...) $k = k_r \text{ mod } l_r^{er}$ para encontrar a

3.3. Método Baby Step Giant Step

Esse método, desenvolvido por Shanks (1971), resolve o problema do logaritmo discreto em \sqrt{n} passos armazenando \sqrt{n} valores. O algoritmo a seguir, baseado em Barker (2008), mostrada como aplicá-lo ao problema do logaritmo discreto sobre curvas elípticas:

Entrada: Curva elíptica $E(F_p)$, ponto base P de ordem n , chave pública Q .

Saída: Chave privada k .

1. Selecionar $m \in \mathbb{Z}$ de forma que $m \geq \sqrt{n}$ e calcular $m * P$.
2. Cria uma lista $T = \{i * P \mid 0 \leq i < m\}$.
3. Para j de 0 até $m - 1$
 - 3.1. Calcular $Q' = Q - j * m * P$.
 - 3.2. Se houver na lista T um elemento $i * P$ tal que $i * P = Q'$,
retornar: $k = i + i * m \text{ mod } n$.

4. Proposta de Fortalecimento do Esquema de Curvas Elípticas

4.1. Introdução

O objetivo aqui é propor uma forma de fortalecer a criptografia com curvas elípticas. Para isso, será introduzida uma maneira de utilizar rotações ao redor do eixo x , de forma que se possa mascarar os pontos da curva. Em seguida, será proposto um método de criptografia para trabalhar com essas rotações.

4.2. Rotação espacial de uma curva elíptica

Um ponto pode ser rotacionado ao redor dos eixos x , y ou z , através de uma matriz de rotação. Os pontos de uma curva elíptica serão rotacionados ao redor do eixo x , através da matriz de rotação definida a seguir.

Definição 3: Dado um ponto $P = (x, y, z)$, o ponto rotacionado ao redor do eixo x $P' = (x, y', z')$, com um ângulo θ , é dado por $P' = R_x * P$, onde R_x é a seguinte matriz de rotação:

$$R_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix}$$

Para reverter esta transformação, basta multiplicar P' pela matriz transposta, isto é, $P = P'^*R_x^T$.

Para manter as coordenadas dos pontos da curva elíptica no conjunto dos números inteiros, serão usados quatro tipos de rotações: 0° , 90° , 180° e 270° . Dessa forma, cada ponto (x, y) da curva elíptica, depois de rotacionado, terá quatro possibilidades: $(x, y, 0)$, $(x, 0, y)$, $(x, -y, 0)$ e $(x, 0, -y)$.

4.3. Como usar a rotação para aumentar as possibilidades de criptografia

O objetivo aqui é, através das rotações, tentar mascarar os pontos da curva elíptica.

Um ponto (x, y) rotacionado 270° , por exemplo, é representado como $(x, 0, -y)$. Ao analisar-se esse ponto sem saber a rotação que foi aplicada a ele, tem-se duas possibilidades ambíguas de sua origem: $(x, 0, y)$ e $(x, 0, -y)$.

Os pontos rotacionados serão representados da seguinte forma: se o ponto for do tipo $(x, 0, z)$, ou seja, se ele estiver no plano xz , ele será representado como $(x, -z, z)$. Caso ele seja do tipo $(x, y, 0)$, ou seja, se ele estiver no plano xy , ele será representado como $(x, y, -y)$. Para devolver o ponto ao seu plano original, basta igualar sua componente z a zero, caso a rotação tenha sido de 0° ou 180° , ou igualar sua componente y a zero, caso a rotação tenha sido de 90° ou 270° . A figura 1 ilustra esse procedimento.

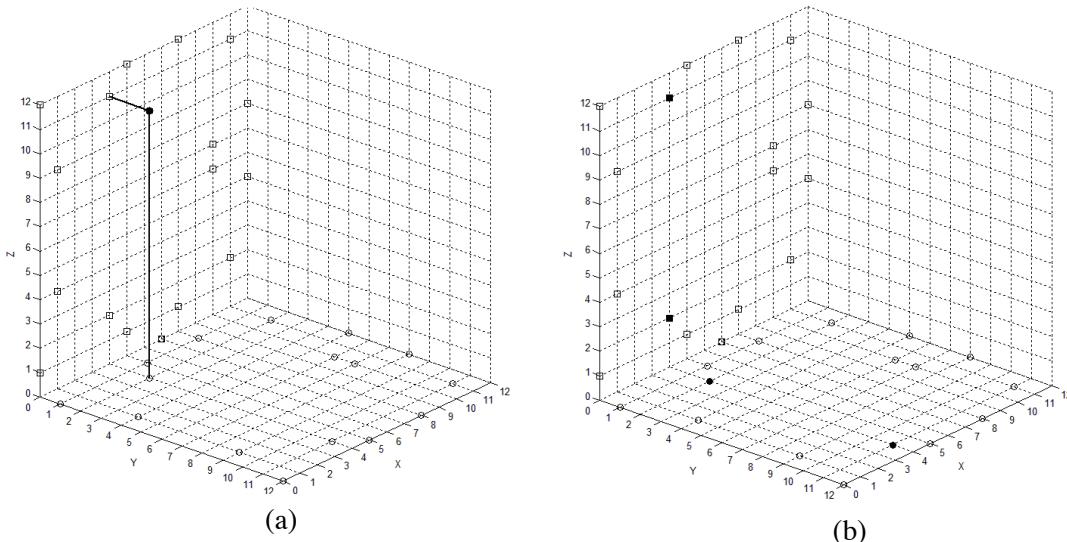


Figura 1: (a) Ponto rotacionado e projetado para fora dos planos. (b) Os quatro pontos referentes às possíveis origens da rotação e projeção.

4.4. Método de Criptografia Proposto

Agora, será definido um novo método que utiliza rotações em torno do eixo x para aumentar a segurança do método de curvas elípticas.

Será necessário escolher o tipo de corpo que será utilizado, os parâmetros da curva elíptica E , um ponto base $P \in E$. As chaves públicas, porém, serão definidas de uma maneira diferente. Além de escolher uma chave privada s , cada usuário desse sistema deverá escolher uma rotação R' para aplicar ao ponto P , obtendo o ponto P' . Então, a chave pública Q' será o ponto sP' . Será necessário, também, um segundo par de chave pública e chave privada, portanto cada usuário deverá ainda escolher outro número para ser sua chave privada n , e multiplicar por P , obtendo a segunda chave pública Q .

Agora, será mostrado como a rotação que será utilizada no envio de mensagens é definida. Cada uma das possíveis rotações deve ser atribuída a um ponto na curva. Então, basta enviar o ponto referente à rotação R escolhida através do método de ElGamal, utilizando a segunda chave pública definida pelo outro usuário.

Após se ter definido a rotação R , o envio de mensagens será feito da seguinte forma: primeiro, deve-se aplicar a rotação R às duas possibilidades da chave pública do destinatário, obtendo Q'' e Q''' . Deve-se, também, escolher um inteiro k aleatório. Então, a mensagem $X = (x_1, x_2)$ será enviada através da 4-upla $Y = (y_0, y_1, y_2, y_3)$, que é calculado da seguinte forma:

$$\begin{aligned} \bullet y_0 &= RkP \\ \bullet y_1 &= c_1 x_1 \\ \bullet y_2 &= c_2 x_2 \\ \bullet y_3 &= c_3 x_2 \end{aligned}$$

onde $(c_1, c_2) = kQ''$, $(c_1, c_3) = kQ'''$ e y_0 tem sua coordenada $y = -z$ caso $y = 0$ ou $z = -y$, caso contrário. Para evitar que y_2 seja igual a y_3 , quando a rotação R for de 90° , o y_3 será calculado como $y_3 = c_3(-x_2)$.

Ao receber $Y = (y_0, y_1, y_2, y_3)$, a mensagem $X = (x_1, x_2)$ é recuperada da seguinte forma: primeiro, y_0 deve ser retornado ao seu plano original igualando sua coordenada z a 0. Caso a rotação R seja de 0 ou 180 graus, ou, caso contrário, igualando sua coordenada y a 0. Em seguida, caso o resto da divisão do ângulo de R somado ao ângulo de R' do destinatário por 180 for 0:

$$\begin{aligned} \bullet x_1 &= y_1(c_1)^{-1} \\ \bullet x_2 &= y_2(c_2)^{-1}. \end{aligned}$$

Caso contrário:

$$\begin{aligned} \bullet x_1 &= y_1(c_1)^{-1} \\ \bullet x_2 &= y_3(c_3)^{-1} \end{aligned}$$

onde $(c_1, c_2, c_3) = s^*R'^*y_0$.

Caso a rotação R tenha sido de 90° , $x_2 = -x_2$.

5. Implementação

Agora, serão apresentados trechos de uma implementação em Java do método proposto, começando pela combinação da rotação entre os usuários. Para armazenar os quatro pontos referentes às possíveis rotações, foi criada a lista *lr*. Os pontos armazenados nas posições 0, 1, 2 e 3 correspondem, respectivamente, às rotações de 0°, 90°, 180° e 270°. Para representar a curva elíptica e sua aritmética, foi criada a classe CurvaEliptica. Uma instância dessa classe, chamada *e*, é utilizada para realizar os cálculos.

```
Ponto pm;
Ponto c1, c2;
pm = lr.get(rt);
Random rn = new Random(System.nanoTime());
int k = Math.abs(rn.nextInt()%e.order(p));
c1 = e.multiplica(k, p);
c2 = e.soma(pm, e.multiplica(k, x.getQ1()));
```

Nessa parte do código, são calculados os pontos C_1 e C_2 do método, recebendo como parâmetros o destinatário *x* e o inteiro *rt*, referente à rotação a ser combinada. O ponto *pm*, referente à mensagem a ser enviada, é retirado da posição *rt* da lista *lr*. O inteiro aleatório *k* é calculado usando a classe *Random*, e seu valor é limitado até a ordem do ponto base *p*, pois a partir daí os valores de $k*p$ começam a se repetir. O método *x.getQ1()* retorna a primeira chave pública do usuário *x*.

```
Ponto pd= e.soma(c2, e.invPonto(e.multiplica(x.getN(), c1)));
int r1= lr.indexOf(pd);
```

Aqui, a mensagem é decodificada e armazenada no ponto *pd*, utilizando *x.getN()* para representar a chave privada de *x*. Então, o índice desse ponto na lista *lr* é armazenado na variável *r1*, que representa a rotação que acaba de ser combinada entre os usuários.

A seguir, será mostrada a implementação da troca de mensagens secretas.

```
Ponto3d q3, q4, c1, c2;
q3 = e.rotaciona(r1, new Ponto3d(x.getQ2().getX(), x.getQ2().getY(), 0));
q4 = e.rotaciona(r1, new Ponto3d(x.getQ2().getX(), 0, x.getQ2().getZ()));
c1 = e.multiplica3d(k, q3);
c2 = e.multiplica3d(k, q4);
int k = Math.abs(rn.nextInt()%e.order(p));
```

No trecho de código mostrado na próxima página, são calculados os valores que servirão de base para criar a quádrupla *Y*.

```
Ponto3d y0= e.rotaciona(r1, e.multiplica(k, p));
int y1, y2, y3;
if (r1 == 0 || r1 == 2) {
    y0.setZ(e.calcMod(-y0.getY()));
    y1 = e.calcMod(c1.getX() * px.getX());
    y2 = e.calcMod(c1.getY() * px.getY());
    y3 = e.calcMod(c2.getZ() * px.getY());
} else {
    y0.setY(e.calcMod(-y0.getZ()));
    y1 = e.calcMod(c1.getX() * px.getX());
    y2 = e.calcMod(c1.getZ() * px.getY());
    if(r1==1)
        y3 = e.calcMod(c2.getY() * e.calcMod(-px.getY()));
    else
        y3 = e.calcMod(c2.getY() * px.getY());
}
```

Aqui, os componentes de Y são calculados. O ponto $y0$ é projetado para fora do plano xy ou xz , dependendo da rotação escolhida, e a mensagem px é embutida nos números $y1$, $y2$ e $y3$, utilizando como base os pontos $c1$ e $c2$.

```
Ponto3d c3;
Ponto pd;
if (r1 == 0 || r1 == 2) {
    y0.setZ(0);
} else {
    y0.setY(0);
}
c3 = e.multiplica3d(x.getS(), e.rotaciona(x.getRp(), y0));
if ((x.getRp() + r1) % 2 == 0) {
    x1 = e.calcMod(y1 * e.calclnvd(c3.getX()));
    x2 = e.calcMod(y2 * e.calclnvd(c3.getY()));
} else {
    x1 = e.calcMod(y1 * e.calclnvd(c3.getZ()));
    x2 = e.calcMod(y3 * e.calclnvd(c3.getZ()));
    if(r1==1){
        x2 = e.calcMod(-x2);
    }
}
pd = new Ponto(x1,x2);
```

Aqui, a mensagem é decodificada e armazenada no ponto pd . Inicialmente, o ponto $y0$ é projetado de volta para o plano xy ou xz , de acordo com a rotação combinada. Em seguida, é calculado o ponto $c3$, que é composto pelos números $c1$, $c2$ e $c3$ do método. Finalmente, os componentes de pd , $x1$ e $x2$, são calculados de acordo com $r1$, a rotação combinada, e rp , a rotação privada do usuário que recebeu a mensagem.

6. Testes

Agora, serão realizados testes do método proposto com diferentes parâmetros, utilizando a implementação descrita na seção anterior.

Teste 1: o objetivo desse teste é verificar se o método realiza com sucesso o envio do ponto (629, 347). Para isso, será usada a curva elíptica $E: y^2 = x^3 + 33x + 33$ definida sobre o corpo finito F_{701} . O ponto P foi definido como (470, 82). O destinatário escolheu suas chaves privadas $n = 97$ e $s = 232$, sua rotação $rp = 180^\circ$, e publicou suas chaves públicas $Q = (75, 147)$ e $Q' = (638, 344, 357)$.

A combinação da rotação de 90° é feita através do ponto (697, 347). Esse ponto é codificado nos pontos $(C_1, C_2) = ((286, 137), (30, 191))$. Ao recebê-los, o destinatário os decodifica e encontra o ponto (697, 347) = 90° .

O envio do ponto (629, 347) é feito através da 4-upla $(y_0, y_1, y_2, y_3) = ((682, 87, 614), (483, 563, 138))$. Ao receber esses valores, efetua a decodificação e encontra o ponto (629, 309).

Resultado do teste: O ponto (629, 347) foi codificado, enviado e decodificado com sucesso.

Teste 2: o objetivo desse teste é verificar se o método envia com sucesso uma série de pontos, formando a mensagem "SOS". A curva elíptica a ser usada é a $E: y^2 = x^3 + 87x + 97$, definida sobre o corpo finito F_{1373} . O ponto P foi definido como (1107, 76). O destinatário escolheu suas chaves privadas $n = 399$ e $s = 578$, sua rotação $rp = 0^\circ$, e publicou suas chaves públicas $Q = (1014, 417)$ e $Q' = (661, 1068, 305)$. A letra "S" foi mapeada no ponto (518, 479), e a letra "O" foi mapeada no ponto (518, 894).

A combinação da rotação de 180° é feita através do ponto (1187, 1152). Esse ponto é codificado nos pontos $(C_1, C_2) = ((442, 1318), (677, 1150))$. Ao recebê-los, o destinatário os decodifica e encontra o ponto (1187, 1152) = 180° .

A mensagem "SOS" é enviada através dos pontos (518, 479), (518, 894) e (518, 479). A codificação desses pontos é feitas nas três 4-uplas: $(y_0, y_1, y_2, y_3) = ((1038, 941, 432), (766, 658, 715), ((160, 324, 1049), 492, 633, 740))$ e $((223, 437, 936), 830, 194, 1179)$. Ao receber esses valores, o destinatário os decodifica, encontrando os pontos (518, 479), (518, 894) e (518, 479), que correspondem, respectivamente, às letras "S", "O" e "S".

Resultado do teste: a sequência de pontos foi codificada, enviada e decodificada com sucesso.

7. Conclusões e trabalhos futuros

A criptografia com curvas elípticas baseia-se em uma aritmética que envolve os pontos da curva em um corpo finito, na qual a operação de multiplicação entre um inteiro e um ponto não é reversível. Os métodos de criptografia aproveitam esse fato para associar mensagens a pontos da curva, e combinar esses pontos a um outro ponto de forma que só alguém que possua uma

chave específica consiga desfazer essa operação. Com isso, surge o problema do logaritmo discreto sobre curvas elípticas, isto é, dados os pontos P e $Q \in E(F_p)$, encontrar um inteiro k tal que $kP = Q$. Evidências apontam ao fato de que esse problema seja intratável, apesar de não existirem provas matemáticas que comprovem isso.

A proposta apresentada nesse trabalho apresenta a vantagem de incluir um novo fator aleatório ao método, a rotação. Dessa forma, é criada uma ambiguidade na hora de se tentar quebrar a chave pública Q' , pois não se sabe exatamente qual é a rotação aplicada ao ponto P para tentar resolver $sP' = Q'$. As mensagens enviadas também se tornam mais difíceis de serem quebradas individualmente, pois ainda há uma outra rotação envolvida nesse processo, que deve ser combinada em segredo entre os usuários. O fato dessas rotações serem simples de se calcular também é uma vantagem, pois dessa forma o método não tem sua complexidade aumentada de forma significativa. Outra vantagem é o fato do método de envio de mensagens estar desacoplado do método de estabelecimento de rotações em comum, dando uma liberdade para que os usuários combinem novas rotações sem afetar o envio de mensagens.

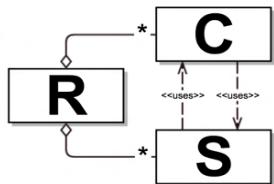
Existem, porém, algumas limitações relacionadas ao método proposto. Uma delas é a necessidade de se estabelecer uma rotação em comum entre os usuários, e isso deve ocorrer em segredo. Esse procedimento é feito utilizando-se um método clássico de criptografia com curvas elípticas, tornando-o vulnerável aos métodos de criptoanálise. Outra limitação é o fato dessa rotação servir apenas para um par de usuários. Por exemplo, se Bob estiver recebendo mensagens de cem usuários diferentes e perder a rotação combinada de um deles, ele não poderá decifrar as mensagens recebidas desse usuário e deverá estabelecer uma nova rotação em comum. Existe, também, a limitação de rotações possíveis. Devido ao fato da aritmética que envolve os pontos das curvas elípticas servir apenas para números inteiros positivos, qualquer rotação que colocar as coordenadas dos pontos no conjunto dos números reais necessitará de um tratamento especial, pois qualquer adaptação nos cálculos estará sujeita a erros de precisão e arredondamento.

Um possível trabalho futuro seria explorar outras formas de transformação que podem ser aplicadas a um ponto e estudar as possíveis formas de utilizá-las para fortalecer a criptografia com curvas elípticas. Novas formas de representar os pontos da curva também podem ser exploradas para esse fim, mas é possível que seja necessário realizar adaptações na aritmética para que se possa trabalhar com essas alterações.

Outra possibilidade de trabalho futuro seria uma implementação do método proposto em hardware. A aritmética em corpos binários é mais fácil de ser implementada em hardware, tornando essa uma boa oportunidade para se realizar uma adaptação no método proposto para trabalhar com curvas elípticas definidas sobre os corpos binários, isto é, do tipo F_{2^m} .

Referências Bibliográficas

- BARKER, Nathan. "Elliptic Curves, Factorization and Cryptography". University of Durham, 2008.
- ELGAMAL, Taher. "A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms". California, 1985.
- HANKERSON, Darrel; MENEZES, Alfred; VANSTONE, Scott. "Guide to Elliptic Curve Cryptography". New York:Springer-Verlag, 2004.
- LAMB, Nicolas. "An investigation into Pollard's Rho method for attacking Elliptic Curve Cryptosystems". 2002.
- POHLIG, S.; HELLMAN, M". An Improved Algorithm for Computing Logarithms Over GF(p) and its Cryptographyc Significance". *IEEE Transactions on Information Theory*. n. 24, p. 106-110, 1978.
- POLLARD, J. M. "Monte Carlo methods for index computation mod p". *Mathematics of Computation*. v.32, n. 143, p. 918-924, 1978.
- SHANKS, D. "Class number, a theory of factorization and genera". *Proc. Symp. Pure Math.* v. 20, p. 415–440, 1971.
- WONG, David. "Elliptic Curves, Cryptography and Factorization". Department of Mathematics–Durham University, 2009.



Framework de Interface Gestual para Windows Phone 7

Hugo F. De Campos, Gabriel M. Matsuda, Ricardo M. dos Santos, Luciano Silva

Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
 Caixa Postal 930 – 01302-907 – São Paulo – SP – Brazil

hugofcampos@gmail.com, gabriel.matsuda@gmail.com,
 ricardo.machezini@gmail.com, luciano.silva@mackenzie.br

Abstract. The Gesture Interface field is one of the most promising fields in Human-Computer Interaction research area. Nowadays, the number of people that have access to computer devices is rising incredibly. This level of access to technology creates the need of having new methods that allow the interaction between the user and the application and also, that this interaction to be done intuitively, in way that the user should not need any previous knowledge. Everyday new technologies are created and these technologies provide new means of interaction. It makes that the treatment of these new technologies becomes even more wide and complex. This work proposes the development of a framework to the Microsoft Windows Phone 7 platform, in order to help the development of electronic games that implement the Gesture Interface. A tool that allows to automate the process of detection, treatment and handling of gestures, such as touch and accelerometer, improving the game development process, using the Microsoft XNA Framework.

Resumo. O campo Interfaces Gestuais é um dos campos de pesquisa mais promissores da área de Interação Humano-Computador. Atualmente, o número de pessoas com acesso a dispositivos computacionais cresce incrivelmente. Tanto acesso a tecnologia cria a necessidade de novas formas de fazer com que o usuário interaja com a aplicação e que seja feito uma forma intuitiva que não necessite de conhecimento prévio do usuário. A cada dia novas tecnologias são criadas e elas disponibilizam novos meios de interação. Isso faz com que o tratamento desses recursos se torne mais amplo e complexo. Neste trabalho, propõe-se o desenvolvimento de um framework para a plataforma Microsoft Windows Phone 7, para auxiliar no desenvolvimento de jogos eletrônicos que implementem Interfaces Gestuais. Uma ferramenta desse tipo permite automatizar o processo de detecção, tratamento e manipulação de gestos, por exemplo de gestos do tipo toque e acelerômetro, facilitando e organizando o processo de desenvolvimento de jogos, utilizando como base o XNA Framework.

1. Introdução

Dentro da área de Interação Humano-Computador, um dos campos de pesquisa mais promissores é o de Interfaces Gestuais. À medida que surgem novas tecnologias em termos de *hardware* para interação entre o homem e a máquina, surgem também novas formas de interagir com o computador. Interface Gestual é a técnica que permite ao usuário interagir com computadores usando os movimentos de seu corpo.

Na área de jogos eletrônicos, a jogabilidade é um dos requisitos mais importantes a serem considerados para o desenvolvimento do jogo. Em plataformas convencionais de jogo, como Playstation e XBOX, a interação do jogador com o jogo é feita por meio de dispositivos de *hardware* específicos para controle (*joysticks*). Já em plataformas não convencionais, em que não existe um dispositivo *hardware* específico, uma boa Interface Gestual deve ser aplicada para se obter uma boa jogabilidade.

Em dispositivos móveis, diversas tecnologias são utilizadas para a interface de controle de usuário. Em especial, dispositivos de telefonia móvel são exemplos dessa aplicação e representam um mercado crescente de aquisição pela popularização dos *smartphones*. Essa plataforma ganhou notoriedade após o lançamento do primeiro modelo do iPhone, da Apple, que substituiu os teclados numéricos ou do tipo “Querty” por um conjunto de sensores que proporcionavam maior interação com os usuários. Desses sensores, destacavam-se a tela sensível ao toque e o acelerômetro. Após a introdução desse conceito, diversas outras plataformas surgiram com a mesma proposta, das quais se destacam os celulares com sistema operacional Android e, mais recentemente, Windows Phone 7.

Com a popularização dos *smartphones*, o mercado de jogos para essa nova plataforma se torna cada vez mais explorado. E dado a constante evolução dos equipamentos, em relação aos seus recursos tecnológicos de entrada de usuário, principalmente sensores, a utilização desses recursos foi tomada como cenário para este trabalho.

O objetivo deste trabalho é a criação de um *framework*, baseado no XNA Framework da Microsoft, para automatizar a detecção, o tratamento e a manipulação de gestos a fim de facilitar o desenvolvimento de jogos para a plataforma Windows Phone 7. O XNA Framework atualmente não fornece componentes nativos, já agregados para detecção, tratamento e manipulação de gestos. Portanto, um *framework* que automatizasse esse processo possibilitaria a abstração da lógica de tratamento de gestos da lógica do jogo em si, aumentando a organização e coesão do código do jogo.

2. Interfaces Gestuais

Na busca da maior interatividade entre jogos eletrônicos e seus jogadores, requisito fundamental para o sucesso do jogo, dois fatores se fazem indispensáveis: a plataforma e a técnica de controle.

A plataforma representa o tipo de equipamento em que este jogo será reproduzido. Pela plataforma define-se qual será o ambiente que o jogador deverá ser inserido para a prática do jogo. Esse aspecto implicará, invariavelmente, nas primeiras restrições em relação ao tipo de controle que será utilizado. Uma plataforma fixa,

como um console, por exemplo, pode impor uma restrição ao número de jogadores simultâneos por uma questão espacial. Da mesma maneira, uma plataforma que utiliza movimentação deverá sofrer limitação na utilização do espaço para o jogo.

A técnica diz respeito a como o jogo irá coletar as informações do jogador para a interação com o ambiente virtual do jogo. Semelhante ao que acontece com a plataforma, a técnica representa outro conjunto de restrições em relação ao jogo. Um controle feito por botões, por exemplo, tem a limitação de número e complexidade de combinações que podem ser feitas. Já jogos que utilizam movimentação devem levar em consideração a natureza do movimento e a viabilidade de utilizá-lo em relação ao espaço físico.

A partir da análise desses dois pontos, é possível estudar a melhor forma de interação entre jogador e jogo. Em particular, este trabalho empenha-se na utilização de gestos para a interação. Para isso, será utilizado o conceito de Interface Gestual, que estuda o comportamento de gestos na interação Humano-Computador. Definir o que é um gesto é algo que muitos pesquisadores tentaram fazer de diversas formas. Todos dizem saber o que um gesto é, mas nenhum pôde definir precisamente o que é [Corradini & Cohen, 2002]. Os movimentos de um corpo definem um aspecto do que é um gesto, embora a maioria das definições tente separar gestos de outros tipos de movimentação humana.

Interface Gestual é a interface do computador que permite ao usuário interagir com computadores usando os movimentos de seu corpo [Cheng et al., 2011]. É um dos campos mais promissores para pesquisadores da área de Interação Humano-Computador, pois faz com que o computador responda melhor as habilidades de cada pessoa, fazendo assim o uso mais intuitivo e prazeroso do que o padrão *mouse* e teclado. Como exemplos de aplicações de interfaces gestuais, pode-se ter:

- **Reconhecimento de *pointing directions*:** por meio de uma câmera, o robô capta as imagens do ambiente, reconhece a posição das mãos e da cabeça do usuário e assim consegue estimar a direção para onde este está apontando [Nickel & Stiefelhagen, 2007], conforme mostra a Figura 1:

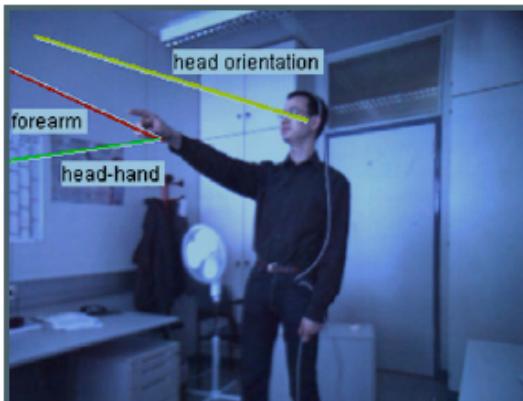


Figura 1: Diferentes abordagens para estimar a *pointing direction*.

Fonte: Nickel & Stiefelhagen, 2007.

- **Reconhecimento de expressões faciais:** por meio de uma câmera, o robô capta as imagens do rosto do usuário, extrai as características faciais e então classifica as expressões em um tipo [Huang & Lin, 2008], como mostra a Figura 2, próxima página.

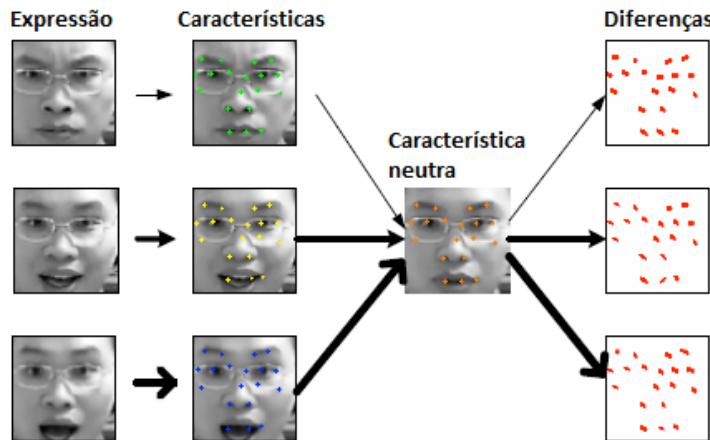


Figura 2 – Diferenças entre expressão facial neutra e outras expressões

Fonte: Huang & Lin, 2008.

3. Interfaces Gestuais aplicadas a Jogos Eletrônicos

Conforme descrito na seção anterior, dois fatores são decisivos para o sucesso de um jogo eletrônico do ponto de vista de interatividade entre o jogador e o jogo: a plataforma e técnica de controle.

O objetivo desta seção é apresentar alguns exemplos de jogos eletrônicos de plataformas atuais e destacar as formas com as quais as aplicações de interfaces gestuais foram aplicadas para solucionar o problema da interação entre o jogador e o jogo eletrônico.

3.1. Brothers In Arms® Hour of Heroes

Neste jogo de tiro em terceira pessoa para iPhone, o jogador controla um soldado avançando pelo campo de guerra. Na tela *multitouch*, além do botão de tiro, é apresentado um *joystick* virtual com o qual o jogador consegue controlar os movimentos do personagem pelo cenário. Ao tocar nas outras partes da tela o jogador consegue alterar a posição da câmera [Gameloft, n.d.].

A Figura 3 mostra uma das telas do jogo Brothers In Arms:



Figura 3 – Brothers In Arms® Hour of Heroes

Fonte: Gameloft, n.d.

3.2. Rise of Glory

Este jogo para Windows Phone 7, tem por objetivo realizar diversas missões, que podem ser do tipo ir de um determinado ponto a outro, passar por um conjunto de anéis (*checkpoints*) em um tempo determinado, e destruir aviões inimigos [Microsoft, Rise of Glory, n.d.].

O controle do jogo é dividido em dois, uma parte pela interface *touch* que controla as armas e funções básicas do avião, como ligar e desligar o motor. A outra parte é feita por acelerômetro, que controla o manche do avião conforme a movimentação do próprio aparelho. Rotacionar o *smartphone* em relação à tela nos sentidos horário e anti-horário, faz com que o avião gire em torno de seu próprio eixo. Já ao incliná-lo para frente e para trás, faz com que o avião empine ou mergulhe.



Figura 4 – Rise of Glory

Fonte: Microsoft, n.d.

4. XNA Gesture Interface Framework

Nesta seção é proposto um *framework* que tem como objetivo disponibilizar ao usuário que procura desenvolver jogos para plataforma Windows Phone 7 um conjunto de ferramentas que automatize a detecção, o tratamento e a manipulação de gestos para ser utilizado durante a lógica de programação do jogo.

Para isso, antes da implementação, foi necessário fazer um estudo para levantar os requisitos e identificar como o *framework* seria elaborado.

4.1. Requisitos do *Framework*

Assim como em todo desenvolvimento de *software*, para o desenvolvimento do *framework* proposto por este trabalho foi necessário definir os requisitos. A lista a seguir mostra os requisitos finais propostos para o *framework*.

- Reconhecer gestos pré-estabelecidos por uma biblioteca de suporte;
- Ser capaz de armazenar e reconhecer uma sequência de gestos;
- Ser capaz de guardar o último gesto reconhecido;
- Possibilitar ao usuário estender o próprio *framework* para implementação do jogo utilizando os recursos disponibilizados pelo *framework*;

4.2. Diagrama de Classes

Nesta seção apresentamos o diagrama de classes do *framework* desenvolvido juntamente com a descrição de cada classe:

- **Gesture:** Classe que denota o gesto genérico para o sistema, sendo extensível para que a implementação dê cobertura para qualquer tipo de gesto seja ele de um tipo *touch* ou de uma leitura do acelerômetro.
- **State:** Classe que denota o estado atual do dispositivo, para que seja possível a compreensão de gestos complexos ou sequenciais, como por exemplo, *double tap* e *pinch*.
- **Manager:** Gerenciador de recursos do *framework* contém a inicialização do sistema e mantém a referência dos membros essenciais para o *framework* (*Gesture List*, *State*, *ActionMediator* e *Monitor*).
- **GestureList:** Classe que lista as ações aceitas pelo sistema, contém as ferramentas para a manipulação da mesma, é necessária para suportar gestos sequenciais ou complexos, como por exemplo, *double tap* e *pinch*.
- **ActionMediator:** Classe que recebe os dados de entrada, e faz todo o trabalho de tratamento daquela entrada, ou seja, é a classe que toma a ação quando um

gesto é obtido pelo sistema, e faz a atualização do estado do sistema de acordo com os gestos válidos aceitos.

- **Monitor:** Classe que espera o evento, quando o evento ocorre o Monitor repassa para que este evento seja tratado pela classe Mediator.

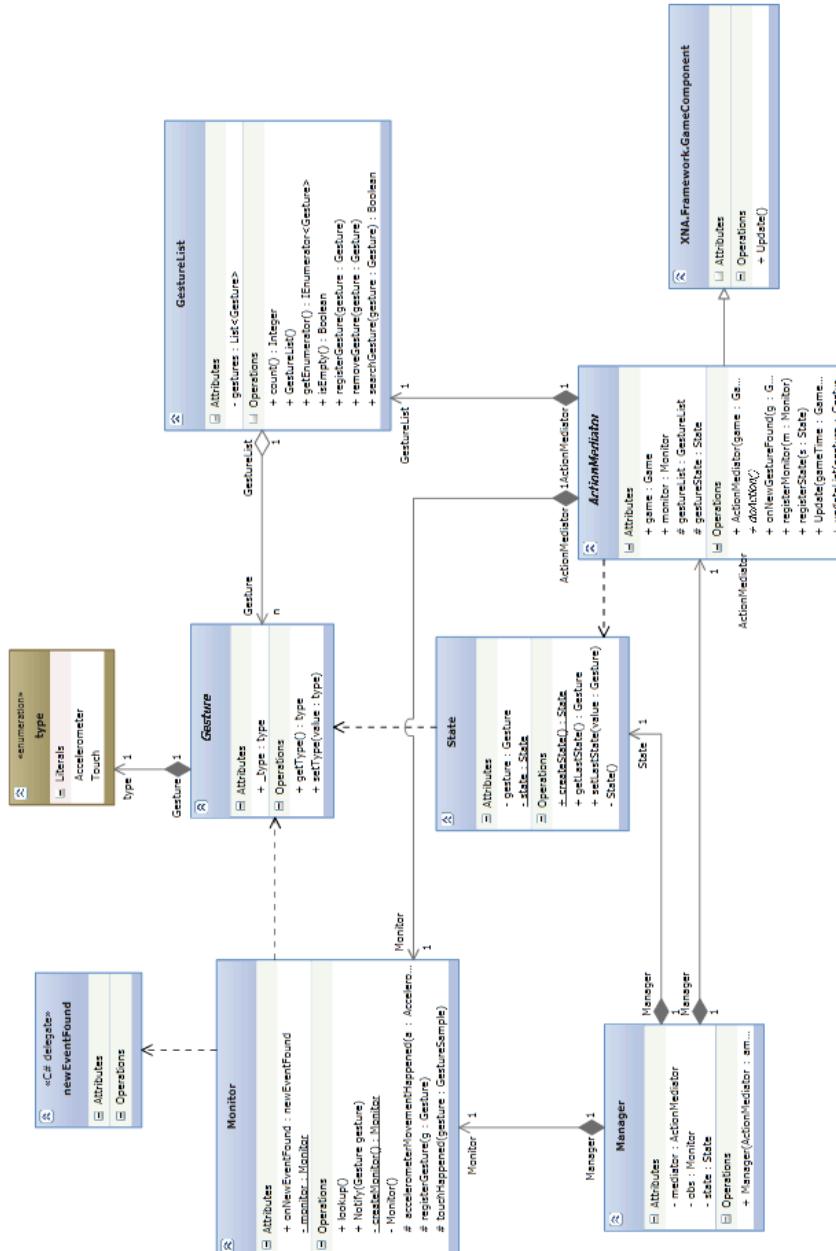


Figura 5 – Diagrama de Classes

4.3. Diagramas de Sequência

Nesta seção, são apresentados os diagramas de sequência do *framework* proposto. O primeiro diagrama, apresentado a seguir, mostra a sequência na qual os componentes do *framework* são instanciados a partir do início para a monitoração de gestos que serão capturados pelo *framework*.

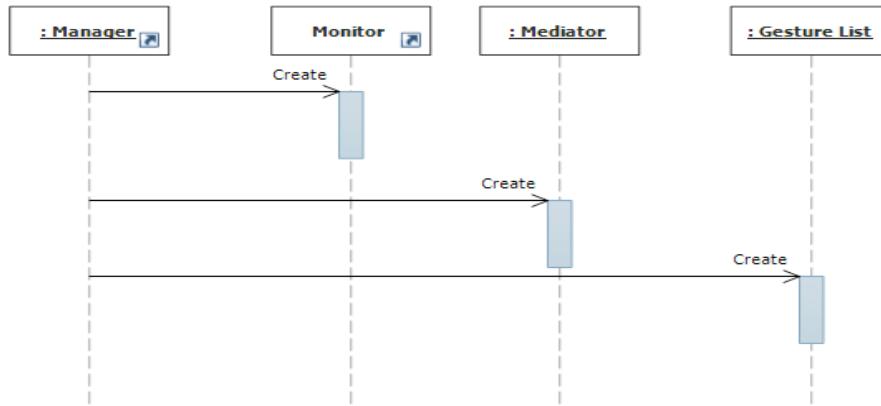


Figura 6 – Diagrama de Sequência I

O Manager é o primeiro componente a ser instanciado, tendo como única função instanciar os demais componentes para o funcionamento do *framework*. Logo após ser criado, o Manager cria o Monitor que será responsável por receber as interrupções geradas pelas interfaces do dispositivo. Em seguida, cria o Mediator que é responsável por receber os gestos do Monitor e fazer a chamada das ações que serão relacionadas a cada gesto. O Mediator também é responsável por atualizar a lista de gestos e o estado do *framework*. Por fim, o Manager cria a GestureList que é a estrutura que irá armazenar os gestos capturados pelo Monitor e registrados pelo Mediator.

O próximo diagrama mostra a sequência que o *framework* segue após ser inicializado pelo Manager para fazer o tratamento do gesto a partir de sua leitura.

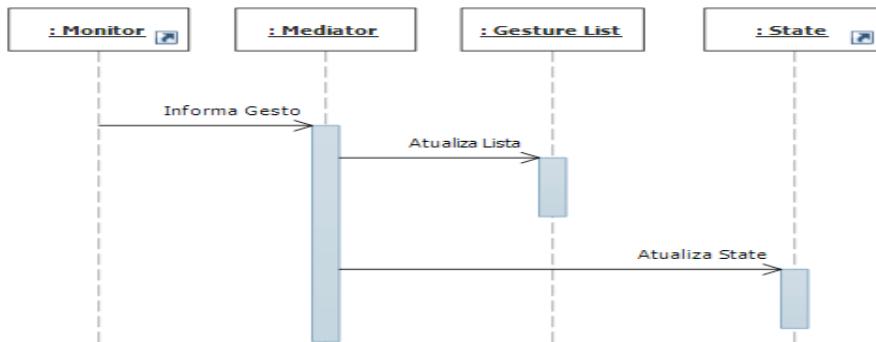


Figura 7 – Diagrama de Sequência II

A técnica proposta para o desenvolvimento do *framework* para fazer a detecção dos gestos foi a técnica de *Polling*. A técnica de *Polling* consiste em fazer com que o próprio sistema verifique regularmente cada dispositivo para obter a informação necessária para processamento [Tanenbaum & Woodhull, 2000]. Porém como a proposta inicial do *framework* é monitorar somente dois recursos do dispositivo (tela *multitouch* e acelerômetro) e devido à facilidade de implementação, a técnica de *Polling* foi escolhida.

Após receber o gesto monitorado pelo sistema, o Monitor informa o gesto ao Mediator. Este por sua vez faz a chamada das ações que serão relacionadas a cada gesto, conforme programado pelo usuário que faz a extensão do *framework*. O Monitor também é responsável por realizar a inserção do gesto na lista de gestos e fazer a atualização do estado do *framework*.

5. Implementação

A implementação foi baseada no XNA Framework da Microsoft. O *framework* desenvolvido foi criado como uma *library* para XNA. Dessa maneira ele poderá ser importado em qualquer projeto do para a plataforma Windows Phone 7 utilizando XNA Framework.

O ambiente de desenvolvimento utilizado para a produção do *framework* foi o Visual Studio 2010, juntamente com o Windows Phone SDK e o XNA Game Studio 4.0.

5.1. Generalização dos gestos

A primeira estrutura criada foi a classe *Gesture*, que generaliza a manipulação de qualquer interação com o dispositivo. Essa classe se utiliza de uma enumeração para determinar qual o tipo de origem de sua criação, permitindo a recuperação posterior de sua estrutura original.

Para o desenvolvimento desse trabalho, foram abordados as entrada *Touch* e *Accelerometer*, ambos fornecidos nativamente pelo XNA Framework. A escolha desses dois elementos se deve a serem comumente usados em aplicações para dispositivos móveis, principalmente para jogos.

```
public abstract class Gesture
{
    private type _type;

    public type Type
    {
        get { return _type; }
        set { _type = value; }
    }
}
```

A classe abstrata Gesture permite que diversos mecanismos de entrada sejam tratados de maneira genérica. Para isso, é necessário apenas criar uma nova classe que estenda a classe Gesture e que dê suporte a essa nova entrada.

O método público Type é responsável por informar o tipo de gesto encapsulado pelo objeto e será utilizado principalmente para o posterior tratamento desse gesto pela classe ActionMediator.

5.2. Detectando os gestos

O primeiro passo para a identificação do evento é detectá-lo. Os dispositivos móveis com Windows Phone 7 possuem diversas interfaces de interação, como tela sensível a toque, acelerômetro, bússola, etc.

A classe Monitor dispõe de um mecanismo que dá ao utilizador do framework a possibilidade de utilizar qualquer tipo de entrada de dados, delegando a responsabilidade de manipulação da lista ao framework.

```
public class Monitor
{
    public delegate void newEventFound(Object sender, Gesture g);
    public newEventFound onNewEventFound;

    protected void registerGesture(Gesture g)
    {
        if (onNewEventFound != null)
        {
            onNewEventFound(this, g);
        }
    }

    public void lookup()
    {
        //... implementação da lógica de detecção dos gestos
    }
    //...
}
```

A construção da classe possui um atributo do tipo *delegate*, o newEventFound, responsável por determinar a assinatura do método que poderá ser disparado pelo acontecimento de um gesto. Esse atributo *delegate* será configurado pela instância da classe ActionMediator, que adiciona um método

próprio ao atributo, dizendo que seu método `onNewGestureFound()` será responsável pelo tratamento do gesto encontrado.

Para a detecção de um gesto, o mecanismo proposto utiliza o método `lookup()`. Esse método possui a lógica de detecção das entradas de usuário, que devem ser analisadas e, se assim decidir, enviadas para tratamento do *framework*.

O método `registerGesture` é chamado quando uma entrada de usuário foi detectada. Sua responsabilidade é repassar a chamada ao método configurado pelo atributo `delegate` da classe `Monitor`. Dessa forma, o tratamento desse gesto é delegado ao `ActionMediator`.

5.3. Manipulando os gestos

Para tratar uma grande quantidade de elementos do tipo `Gesture`, foi criada a classe `GestureList`, que contém mecanismos que manipulam uma lista de gestos sequenciais.

```
public class GestureList
{
    private List<Gesture> gestures;

    public GestureList()
    {
        gestures = new List<Gesture>();
    }

    public IEnumerator<Gesture> GetEnumerator()
    {
        foreach (Gesture g in this.gestures)
        {
            yield return g;
        }
    }
}
```

A implementação foi feita utilizando um objeto do tipo `List` para manter todos os gestos encontrados. Foram definidos então, os métodos para a manipulação dessa lista, responsáveis por inserir, remover e contar elementos contidos por ela. Há disponível, também, o método `GetEnumerator`, que foi sobreescrito para que a classe pudesse ser iterada de maneira simplificada pela aplicação.

A estrutura responsável por manipular os gestos armazenados é a classe `ActionMediator`. Trata-se de uma classe abstrata que deve ser reescrita pelo utilizador do *framework* e que herda as características da classe `GameComponent` do XNA Framework, podendo por esse motivo ter sua execução atrelada a do jogo.

```
public abstract class ActionMediator : GameComponent
{
    //... declarações de atributos
    public ActionMediator(Game game) : base(game)
    {
        //... inicializações
    }
    public abstract void doAction();
    //...
}
```

A implementação da classe `ActionMediator`, que estende a classe `GameComponent`, obriga a passagem de um objeto do tipo `Game` em sua instânciação, guardando essa referência em um atributo interno. Isso permite que, quando a classe for estendida e o método `doAction` for reescrito, o usuário terá acesso aos recursos do objeto da classe `Game` que foi passado. Isso é de vital importância para que a interação desejada possa ser repassada aos elementos do jogo.

5.4. Utilizando o Framework

O uso do *framework* é feito por meio do controle realizado pela classe `Manager`. A classe `Manager` tem seu construtor que solicita instâncias de `ActionMediator` e `Monitor` para ser inicializada. Isso se deve ao fato de que tais classes podem (e no caso do `ActionMediator` deve) ser estendidas para se agregar funcionalidade. Sendo assim, o construtor da classe carrega as dependências e faz os ajustes para ligá-las. Isso é feito por meio dos registros de `Monitor` e `State` pela instância da classe `Mediator`. A partir de então, os recursos estarão disponíveis para o funcionamento do *framework*.

```
public class Manager
{
    //... declarações de atributos
    public Manager(ActionMediator am, Monitor m)
    {
        //... inicializações das dependências
    }
}
```

A instanciação de um objeto Manager, portanto, garante o acesso aos recursos fornecidos pelo *framework*. Tendo as dependências criadas, o componente do jogo representado pela instância do ActionMediator pode ser adicionado como componente do jogo:

```
//... dentro de um jogo  
manager = new Manager(this.actionMediator,  
Monitor.createMonitor);  
Components.Add(actionMediator);
```

6. Testes

O *framework* desenvolvido foi aplicado ao sistema InputToyWP7 disponibilizado no App Hub [App Hub, n.d.], que faz uso de entradas de toque e acelerômetro padrão. Para exemplificar o uso do *framework*, o sistema de entrada padrão foi substituído utilizando *framework* desenvolvido. Este teste foi submetido em um emulador do sistema do Windows Phone 7, desenvolvido pela Microsoft, com o fim de exibir os aplicativos sem a necessidade de fazer o *deployment* no dispositivo. Como resultado obteve-se: o sistema funcionou da mesma maneira, sem nenhuma deficiência aparente, mas também sem nenhum ganho de desempenho evidente.

A aplicação consiste em uma tela com fundo preto que ocupa todo espaço disponível na tela do dispositivo. Dois botões, ambos acionados por toque, são disponibilizados para o acesso a tela de ajuda e para pausar o a animação. A aplicação espera a interação do usuário por meio de um ou mais toques em qualquer posição de sua tela. No momento que ocorre um toque, na posição onde este foi detectado, deve aparecer uma imagem representando uma fagulha (*sparkle*):

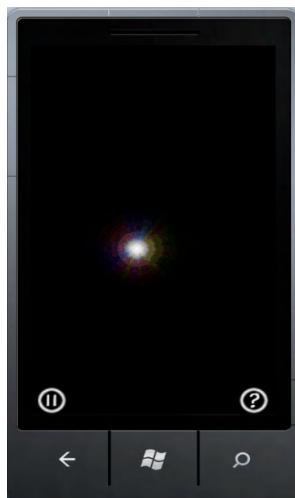


Figura 8 – Imagem da fagulha causada pelo toque

Tendo a referência ao *framework* disponível, a modificação da lógica original pode ser realizada. A aplicação original é implementada sob uma extensão da classe Game, nativa do XNA.

Primeiramente, como é requisito para o uso do *framework*, é necessário a criação de uma classe que estenda a classe ActionMediator, que implementará a lógica da aplicação.

```
Class MyActionMediator : ActionMediator
{
    public MyActionMediator(Game game) :base(game) { }

    public override void doAction()
    {
        Game1 game1 = (Game1)this.game;

        //... implementação da lógica de manipulação dos gestos
    }
}
```

A classe MyActionMediator estende a classe ActionMediator, descrita no *framework*, e é composta por um construtor, que somente chama o construtor da classe pai, e a implementação do método doAction.

O método doAction recebeu toda a lógica de manipulação de gestos implementada pelo jogo original. No método foram feitos os tratamentos de *multitouch*, tanto para a inclusão de novas imagens de fagulha quanto em relação à interação com os botões do menu. No método doAction, os gestos que não foram utilizados pelo método descrito anteriormente, devem ser manipulados para a geração das fagulhas.

Para isso, é criada uma nova instância da classe Sparkle, original da aplicação, passando-se como parâmetro de inicialização as posições do toque, nos eixos X e Y, e o tempo atual do jogo, usado para a animação da fagulha. O tratamento de cada gesto encontrado na lista é iniciado pela verificação da posição do gesto. Isso é necessário para que se encontre gestos localizados sobre os botões da aplicação (*pause* e *help*). Os demais gestos devem ser manipulados para a geração das fagulhas.

Para isso, é criada uma nova instância da classe Sparkle, original da aplicação, passando-se como parâmetro de inicialização as posições do toque, nos eixos X e Y, e o tempo atual do jogo, usado para a animação da fagulha.

Após a implementação da extensão da classe ActionMediator, o *framework* já pode ser usado. Para isso, devem ser criadas as variáveis necessárias para seu funcionamento:

```
Manager manager;
ActionMediator actionMediator;
```

E depois, instanciá-las:

```
this.actionMediator = new MyActionMediator( this );
this.manager = new Manager(this.actionMediator,
Monitor.createMonitor);
Components.Add(this.actionMediator);
```

Nesse ponto é importante notar a criação da instância da classe `ActionMediator`, que recebe a referência `this` como parâmetro. Nesse contexto, a referência `this` representa o próprio jogo e pode ser passada como parâmetro para o `ActionMediator`, que é um `GameComponent`.

Por fim, para que o componente (`ActionMediator`) seja incluído no fluxo de execução do jogo, é necessário adicioná-lo à lista de componentes desse jogo. Como o `ActionMediator` é um `GameComponent`, o XNA Framework permite que o adicione ao atributo `Components`, automatizando esse processo.

Ao final da implementação e dos testes, podemos observar que o *framework* é capaz de detectar, tratar e manipular gestos de forma automática, permitindo ao usuário reescrever a lógica de manipulação dos gestos, e cumpriu o requisito de tratamento de gestos sequenciais, embora não seja capaz de dar suporte a dispositivos como câmera, bússola, microfone, pois estavam fora do escopo do trabalho devido às restrições de tempo para o desenvolvimento.

7. Conclusões e Trabalhos Futuros

Interface Gestual é a interface do computador que permite ao usuário interagir com computadores por meio de gestos. Dentro da área de Interação Humano-Computador é um dos campos de pesquisa mais promissores, buscando novas formas de interação mais intuitivas entre o usuário e o computador.

No mercado de jogos eletrônicos, um requisito fundamental para o sucesso de um jogo é a técnica de controle aplicada. Dessa forma, em plataformas não convencionais de jogos (que não se utilizam de um *joystick*) tais como aparelhos celulares e *tablets*, uma boa Interface Gestual deve ser aplicada para se obter uma boa jogabilidade.

Este trabalho se propôs a apresentar um *framework* que disponibilize ao usuário que procura desenvolver jogos para a plataforma Windows Phone 7 um conjunto de ferramentas que automatize a detecção, o tratamento e a manipulação de um gesto individual ou de uma sequência de gestos durante o jogo. Dessa forma é possível abstrair a lógica de programação de detecção, tratamento e manipulação de gestos da lógica do próprio jogo.

O XNA Gesture Interface Framework, proposto por este trabalho, disponibiliza um conjunto de ferramentas que podem ser adicionadas ao projeto do jogo em forma de uma biblioteca que automatiza a detecção, o tratamento e a manipulação de gestos durante o jogo, um recurso que não era disponível pelo XNA

Framework de maneira centralizada e genérica. Além disso, o XNA Gesture Interface Framework é extensível, permitindo que o usuário adicione novas funcionalidades para novos recursos agregados a plataforma Windows Phone 7 sem a necessidade de se criar um nova versão do *framework*.

O XNA Gesture Interface Framework desenvolvido disponibilizou suporte somente a dois dispositivos de entrada. A plataforma Windows Phone 7 por sua vez, fornece outros recursos nativos, como câmera, microfone, bússola e pêndulo, que podem ser utilizados para detectar gestos. Caso o *framework* seja adaptado aumentando o número de dispositivos suportados, como os citados anteriormente, a aplicação pode sofrer problemas de desempenho, uma vez que o *framework* precisará monitorar vários dispositivos de entrada constantemente, ou seja, a cada *loop* de processamento do jogo.

Uma possibilidade de trabalho futuro é aumentar o número de dispositivos de entrada suportados pelo XNA Gesture Interface Framework. O sistema atual fornece suporte somente a dois recursos (o *touchscreen* e o acelerômetro), porém a plataforma Windows Phone 7 possui os demais recursos nativos que poderiam vir a ser suportados pelo *framework*.

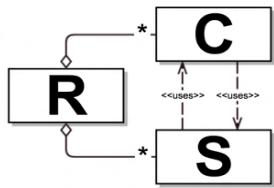
Outra possibilidade de trabalho futuro é a adaptação do XNA Gesture Interface Framework para um sistema baseado em interrupções geradas pelos dispositivos. Essa técnica consiste em deixar que o dispositivo dispare um sinal de interrupção no sistema cada vez em que este necessite de um serviço. Dessa forma o sistema interrompe o processamento corrente e atende a interrupção gerada pelo dispositivo. Essa adaptação forneceria uma melhora de desempenho ao *framework* em relação ao sistema atual baseado na técnica de *Polling*, uma vez que o sistema deixaria de monitorar os dispositivos constantemente, obtendo ganhos em tempo de processamento.

Por fim, mais uma possibilidade de trabalho futuro com base no XNA Gesture Interface Framework apresentado por este trabalho é a mudança do próprio *framework* para outras plataformas, além da Windows Phone 7, que também se utilizem do XNA Framework, como PC e XBOX, dando suporte, por exemplo, ao Microsoft Kinect. A adaptação do *framework* para uma plataforma com mais recursos, como o Microsoft Kinect, possibilitaria agregar outras funcionalidades como captura de gestos por câmera infravermelho e vetor de microfones ao XNA Gesture Interface Framework.

Referências Bibliográficas

- CHENG, H.; CHEN, A. M.; RAZDAN, A.; BULLER, E. (2011). “Contactless Gesture Recognition for Mobile”, In: MIAA 2011.
- CORRADINI, A. e COHEN, P. (2002). “Multimodal Speech-Gesture Interface for Handfree Painting on a Virtual Paper Using Partial Recurrent Neural Networks as Gesture Recognizer”.
- GAMELOFT. Brothers in Arms: Hour of Heroes - Official iPhone Game, Top Action Game for iPhone. Disponível em: < <http://www.gameloft.com/iphone-games/brothers-in-arms-hour-of-heroes/>>. Acesso em: 03 de fevereiro de 2012.

- HUANG, X. e Y, Lin. (2008). “A vision-based hybrid method for facial expression”, In: Ambi-Sys '08: Proceedings of the 1st International Conference on Ambient Media and Systems.
- MICROSOFT. App Hub - Develop for Windows Phone & XBOX360. Disponível em: <<http://create.msdn.com/en-US/>>. Acesso em: 02 de maio de 2012.
- MICROSOFT. Rise of Glory. Disponível em: <<http://www.windowsphone.com/pt-br/apps/c623f41b-af04-e011-9264-00237de2db9e>>. Acesso em: 04 de fevereiro de 2012.
- NICKEL, K. e STIEFELHAGEN, R. (2007). “Visual recognition of pointing gestures for human–robot interaction”, In: Image and Vision Computing, v. 25, n. 12, 2007, p. 1875-1884.
- TANENBAUM, A. e WOODHULL, A. Sistemas Operacionais: projeto e implementação. 2. ed. Porto Alegre: Editora Bookman, 2000.



Implementação de um Circuito Meia-Soma em Sistemas Biomoleculares

Fernando Rodrigues Noronha Héleno, Luciano Silva

Faculdade de Computação e Informática - Universidade Presbiteriana Mackenzie
Caixa Postal 930 – 01302-907 – São Paulo – SP – Brazil
fuheleno@gmail.com, luciano.silva@mackenzie.br

Abstract: This work presents an *in silico* experiment in Molecular Computing. Firstly, it presents the fundamental knowledge needed to understand key structures present in a cell and related methods for information processing involving DNA molecules. After, it has been showed the development of mathematical models capable of converting knowledge existent in the Electrical Engineering field to the Molecular Biology field, making it possible to adapt the ideas of Digital Circuits, actually diffused into hardware based in *silico* technology to a new medium, the biomolecular one. Finally, there is some analysis about the implementation of three logical gates (NOT, AND and XOR) in a biochemical environment and, joining them in a proper manner, the work concludes with a biochemical half-adder circuit and the respective analysis of its simulation.

Resumo: Este trabalho tem o intuito de apresentar um experimento *in silico* na área de Computação Molecular. Inicialmente, é apresentada uma descrição dos principais conhecimentos necessários para se entender as estruturas presentes nas células e os métodos responsáveis pelo processamento de informação contida nas moléculas de DNA. Em seguida, aborda-se o desenvolvimento de modelos matemáticos capazes de converter o conhecimento existente no campo da Engenharia Elétrica para o campo da Biologia Molecular, fazendo possível adaptar as idéias de Circuitos Digitais atualmente difundidas no hardware baseado em silício para um novo meio, o meio celular. Finalmente, é realizada uma implementação de três portas lógicas (NOT, AND e XOR) num ambiente bioquímico e sua devida união para formar um circuito meia-soma, juntamente com a respectiva análise do resultado gerado por processos de simulação neste circuito.

1. Introdução

A base fundamental da vida dos seres vivos está codificada em seu material genético. Suas moléculas de DNA são responsáveis por carregar informações a respeito

do tamanho do ser, cor dos olhos, tipo de formação óssea, entre outras características exclusivas da cada espécie. E, apesar da enorme diversidade existente no mundo em relação a todos esses aspectos, os seres vivos possuem uma coisa em comum, as bases desse material genético são as mesmas para todos. A partir das informações contidas em uma molécula de DNA o embrião passa por uma série de processos bioquímicos, os quais serão responsáveis por expressar as informações contidas nesses genes. Tomando-se então outro ponto de vista, o da Computação, pode-se enxergar uma série de processos algorítmicos capazes de realizar computação, onde os dados de entrada são as informações codificadas nos genes e o encadeamento de processos de tradução, transcrição e replicação genéticos são os passos que o algoritmo deve realizar a fim de obter uma saída computacionalmente aceitável.

A construção de circuitos bioquímicos representa a potencialidade existente em organismos vivos de ser possível aplicar uma forma de controle digital bem conhecida com a finalidade de regular o comportamento celular com alta precisão.

O presente trabalho se propõe a desenvolver um modelo computacional capaz de realizar uma operação binária de soma juntamente com a representação do “carry”, caso exista, compondo assim um Circuito de Meia-Soma bioquímico.

Essa implementação visa, não somente apresentar a possibilidade de se implementar o Circuito Meia-Soma digital em um ambiente biológico, como também demonstrar o quanto controlado pode ser o sistema para que este tipo de implementação seja possível e, a partir deste experimento, dar início a implementação de circuitos mais complexos fazendo uso mais amplo das propriedades celulares como o processamento paralelo e os processamentos em membranas.

2. Fundamentos de Biologia Molecular

Derivada do paradigma da Biologia Molecular, a Computação Molecular apresenta-se como uma nova área interdisciplinar com bases na Biologia e na Computação. Nela todos os aspectos genéticos e metabólicos, como processos de síntese protética, expressão gênica, entre outros, são estudados com a intenção de expandir o conhecimento com relação ao modo como essas ações são tomadas pela célula, ou seja, quais são os mecanismos básicos que ela executa para processar o algoritmo contido em seu interior através do Ácido Desoxirribonucleico (DNA), do Ácido Ribonucleico (RNA) e das proteínas.

2.1. Dogma Central

O fundamento base da Biologia Molecular, conhecido por “Dogma Central da Biologia Molecular”, está relacionado com os processos de como os genes coordenam a síntese de RNA e proteínas e como eles se replicam. Desse modo, tem-se que o DNA é a peça central desse quebra-cabeça bioquímico, seguido de perto pelo RNA e pelas proteínas. Porém é necessário um estudo prévio das moléculas primordiais constituintes dessas macromoléculas para que seja possível um estudo aprofundado de suas características e dos meios que as células utilizam para executar seu processamento em cima delas (VOET; VOET, 2004). A Figura 1, a seguir, mostra, de forma esquemática, a relação existente entre as principais estruturas bioquímicas e as reações responsáveis pela conversão entre elas, onde as setas cheias representam o sentido natural dos processos, enquanto as tracejadas correspondem a operações especiais. Tanto o DNA

quanto o RNA são capazes de promover auto-replicação, e do DNA, através da transcrição, é formado o RNA, que por sua vez, pelo processo de tradução, forma proteínas. Também existe um processo especial de criação de DNA através de uma molécula de RNA, a Transcrição Reversa.

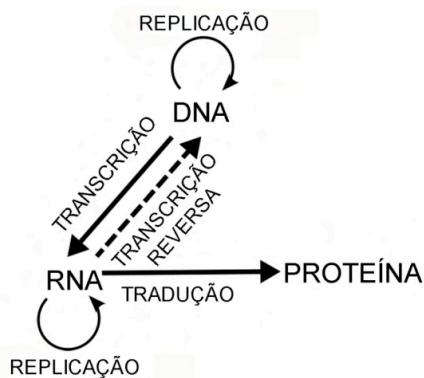


Figura 1 representação esquemática do **Dogma Central da Biologia Molecular**.

Fonte: <http://en.wikipedia.org/wiki/Image:Crick%27s_1958_central_dogma.svg> Último acesso: 28 nov. 2008.

2.2. Nucleotídeos

Os Nucleotídeos são ésteres-fosfato compostos por um açúcar cíclico com 5 átomos de carbono, apresentando uma base nitrogenada no carbono 1' e uma ligação fosfo-éster no carbono 5' (HUNTER).

Quando presentes no DNA, o açúcar que compõe o nucleotídeo é a desoxiribose, enquanto que no RNA é a ribose. Sua diferenciação ocorre no carbono 2', o qual, além de um hidrogênio ligado ao carbono, apresentará um segundo hidrogênio no caso da desoxiribose, ou um grupo álcool (-OH) no caso da ribose fazendo outra ligação com o mesmo carbono (VOET; VOET, 2004). Essas diferenças podem ser visualizadas na Figura 2, na qual é possível observar o carbono 2' e os átomos que diferenciam os compostos; no carbono 5' a presença do grupo fosfo-éster, e no retângulo escrito “Base” é mostrado o lugar onde uma base será anexada.

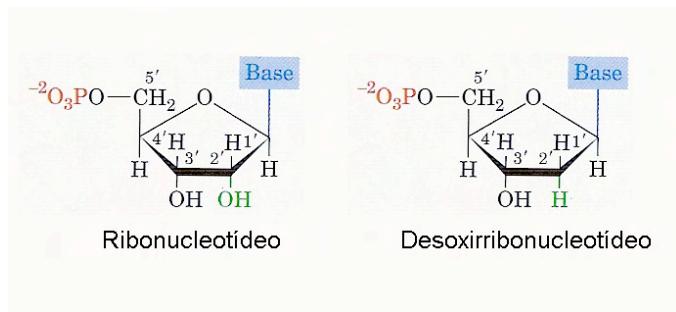


Figura 2 Ácidos nucléicos.

Fonte: VOET, D.; VOET, J.G.(2004, p.81)

Pela definição em Malacinski (2005), as bases nitrogenadas podem ser divididas em dois grupos: as bases púricas – compostas por Adenina (A) e Guanina (G) – e as

bases pirimídicas – compostas por Citosina (C), Timina (T) e Uracila (U). As bases Adenina, Guanina e Citosina estão presentes nos dois ácidos, no entanto a base Timina só está presente no DNA, enquanto a Uracila somente no RNA.

2.3. Aminoácidos

Compostos por um átomo de Carbono, conhecido também por carbono α , ao qual se ligam um grupo carboxila, um grupo amino e uma cadeia lateral, esta formada por cadeias de carbono ou anéis (aos quais se ligam outros grupos funcionais), os aminoácidos são os monômeros formadores das proteínas (VOET; VOET, 2004). Essa estrutura está ilustrada na Figura 4, a seguir.

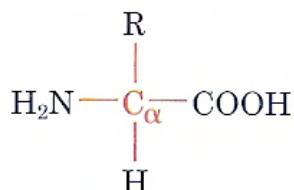


Figura 3 Fórmula estrutural de uma cadeia de um aminoácido representando o átomo de carbono α no centro e os outros grupos funcionais ligados a ele.

Fonte: VOET, D.; VOET, J.G. (2004, p.65)

2.4. DNA

Segundo Malacinski (2005), o DNA apresenta sua composição baseada na Lei de Chargaff. Tal lei afirma que, no DNA, as concentrações das bases A e T são iguais ($[A] = [T]$), assim como as de G e C ($[G] = [C]$). Isso pode ser pressuposto para toda cadeia de DNA de dupla fita, uma vez que A só faz ligações com T e G só faz ligações com C. Essa lei, no entanto, só pode ser provada alguns anos após sua idealização graças a Watson e Crick.

Dessa forma, Malacinski (2005) e Voet e Voet (2004) também afirmam, baseados nas descobertas de Watson e Crick, existir três configurações da molécula de DNA: B-DNA, A-DNA e Z-DNA, porém será estudado apenas o B-DNA, pois este é o mais comum em todos os seres vivos.

B-DNA

Malacinski (2005) e Voet e Voet (2004) definem sua estrutura como sendo duas fitas de polinucleotídeos, as quais são torneadas ao redor de um eixo comum com um giro para a direita, formando uma estrutura em forma de dupla hélice. As duas fitas são antiparalelas, ou seja, tomando um extremo do DNA uma fita apresenta a terminação 3-end enquanto a outra apresenta a terminação 5-end, e não podem ser separadas a menos que se desfaça a forma de dupla hélice.

O plano, o qual contém as bases, é quase perpendicular ao eixo da hélice. A formação desse plano é dada pela ligação de hidrogênio, esta sendo responsável por ligar uma base à outra. Conhecido como Pareamento das Bases, esse fenômeno é o responsável pela associação entre as duas fitas.

Com relação as suas características, o DNA apresenta um comportamento marcante onde ele acomoda apenas dois tipos de bases: a base Adenina se liga apenas com a base Timina assim como a base Guanina se liga apenas com a Citosina, e vice-versa para os dois casos. Essa geometria entre os pares é chamada de Pares de Bases Watson-Crick. Outro detalhe a respeito dessa configuração é que cada base é intercambiável no que diz respeito ao par, ou seja, pode-se inverter as bases do par A·T para T·A sem alterar a posição das estruturas açúcar-fosfato e não é gerado nenhum distúrbio na forma da dupla hélice (MALACINSKI, 2005; VOET; VOET 2004).

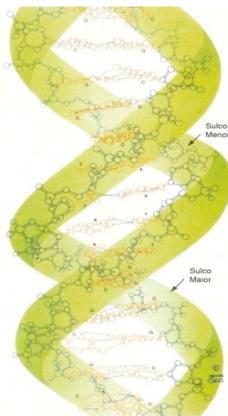


Figura 4 Representação esquemática do B-DNA.

Fonte: VOET, D.; VOET, J.G. (2004, p.1108)

2.5. RNA

Como o DNA, o RNA é uma cadeia polinucleotídica linear, porém seu açúcar é a ribose, ao contrário da desoxirribose presente no DNA; ele apresenta bases U no lugar das bases T do DNA; e, com exceção de alguns vírus e bactérias, o RNA é unifilamentar. Sendo assim, essas moléculas são encontradas no formato de haste-alça ou em formato de grampo, uma vez que as cadeias dobram-se sobre elas mesmas fazendo com que bases complementares se liguem, o que dá origem as alças (MALACINSKI, 2005; VOET; VOET, 2004). A Figura 5, a seguir, trás um exemplo do formato de um tRNA, o qual é responsável por transportar os aminoácidos responsáveis pela codificação das proteínas.

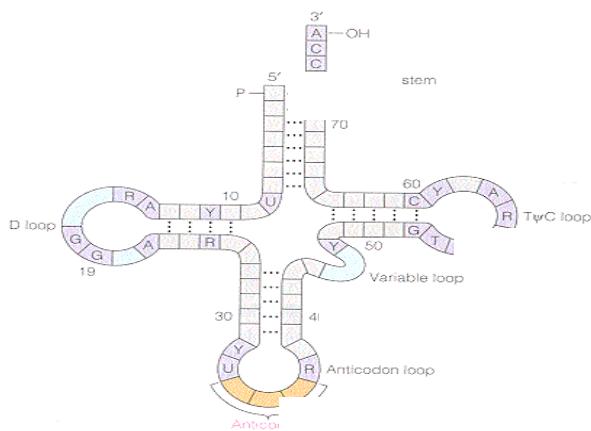


Figura 5 Imagem ilustrativa de um tRNA com seu formato haste-alça e a região do Anticôdon em evidência.

Fonte: <<http://www.cs.stedwards.edu/chem/Chemistry/CHEM43/CHEM43/tRNA/Function.htm>>

Último acesso: 28 nov. 2008

2.6. Replicação de DNA

Segundo Voet e Voet (2004) e Malacinski (2005), para dar-se início à Replicação é necessário que a dupla hélice seja preparada, uma vez que, com os filamentos torcidos, torna-se impossível executar qualquer operação sobre as bases. Esse processo de preparação dos filamentos é composto por 3 partes: a deselicoidização da dupla hélice; quebra das pontes de hidrogênio entre os pares de bases; e separação das fitas e isolamento dos nucleotídeos para que não ocorra uma nova helicoidização antes que as outras enzimas tenham agido.

Após ser preparada a molécula de DNA inicia a Replicação. As proteínas Polimerase I (pol I) e Polimerase III (pol III), responsáveis por polimerizar as fitas-filhas, conseguem realizar seu trabalho apenas no sentido da ponta 5' para a ponta 3', ou seja, apenas uma das fitas será replicada diretamente. A outra, que está invertida em relação a posição inicial da forquilha de replicação, deverá primeiro receber primers (estruturas responsáveis por marcar as posições aonde a pol I deve trabalhar) criados pela proteína Primase, e, em seguida, ela será polimerizada ainda na seqüência da ponta 5' para a ponta 3'. Quando a pol I acaba de polimerizar um pedaço de DNA entre dois primers o resultado dessa polimerização recebe o nome de Fragmentos de Okazaki. Os primers são então substituídos por desoxirribonucleotídeos pela pol I e os fragmentos são unidos para formar a outra fita-filha de DNA. Esse processo está representado na Figura 6.

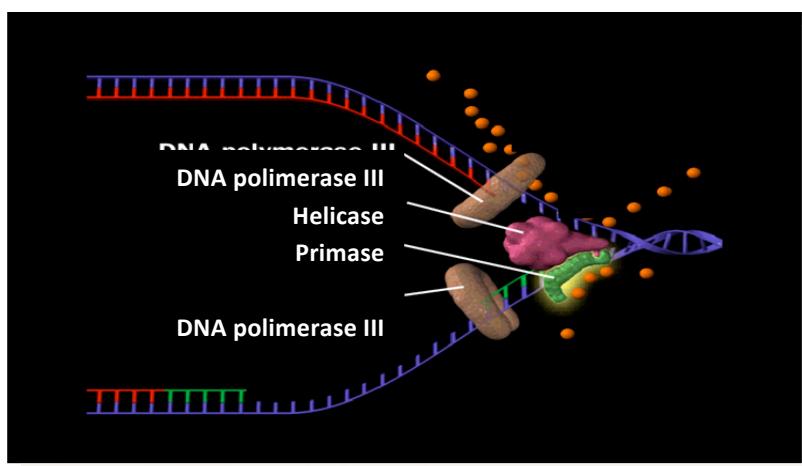


Figura 6 Imagem ilustrativa representando a replicação do DNA.
Fonte: <<http://www.freesciencelectures.com/video/dna-replication-process/>>

2.7. Transcrição

A transcrição é um processo muito semelhante à Replicação. De maneira análoga, uma molécula de DNA é utilizada no processo, enzimas específicas entrarão em ação e uma molécula de RNA será polimerizada. Mas também existem as diferenças, as quais caracterizam esse processo. Em primeiro lugar, o RNA formado é unifilamentar, contrastando com a síntese de um DNA bifilamentar; o filamento de RNA é transcrito de uma parte específica do filamento de DNA, ou seja, não será o filamento inteiro de DNA que será utilizado no processo; e sua enzima de polimerização é a RNA polimerase, uma enzima composta por subunidades sendo que a unidade σ é responsável pela conexão da enzima ao DNA (MALACINSKI, 2005).

A transcrição é constituída por quatro fases. A primeira corresponde a identificação pela proteína RNA polimerase do local apropriado no DNA para ela realizar a transcrição. Esse local é identificado como promotor e contém aproximadamente 40 pares de bases responsáveis por codificar um tipo de identificador para apenas a RNA polimerase certa transcrever aquele pedaço de DNA. A segunda etapa corresponde a Fase de Iniciação. Essa fase representa o início da transcrição pois o primeiro sítio da RNA polimerase, conhecido como sítio de iniciação, tem a característica especial de, geralmente, conter uma Timina ou Citosina, o que gera uma base purínica no início do RNA. A próxima fase conhecida por Fase de Elongação, é responsável pela codificação de todo o resto da cadeia de RNA. Cada vez que um novo aminoácido é ligado ao sítio de elongamento da RNA polimerase, esta move-se uma posição para frente deixando o sítio de elongação livre para uma nova base se conectar. A última fase, também chamada de Fase de Finalização é responsável por terminar a transcrição. Essa fase ocorre quando uma seqüência finalizadora é encontrada pela RNA polimerase. Nesse momento ela processará essa cadeia e ao processar a última base do DNA o RNA se desprenderá por completo dela e ela se desprenderá do DNA (MALACINSKI, 2005; VOET; VOET, 2004). A Figura 7 exemplifica as três últimas fases da Transcrição.

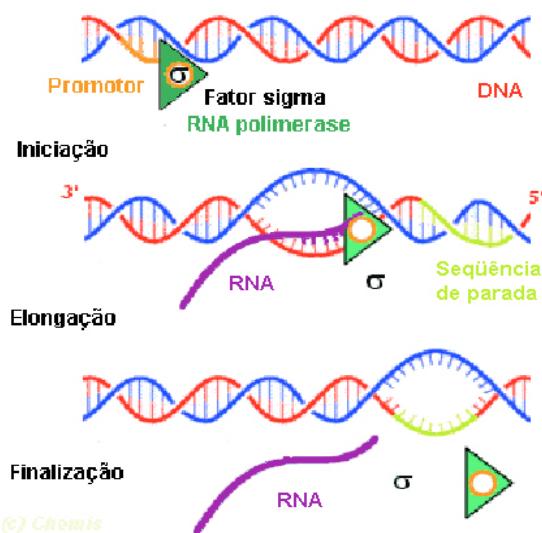


Figura 7 Representação gráfica das três últimas fases da Transcrição.

Fonte: <<http://www.geneticengineering.org/chemis/Chemis-NucleicAcid/RNA.htm>>

Último acesso: 28 nov. 2008

2.8. Tradução

Para Malacinski (2005) e Voet e Voet (2004), tradução é o processo pelo qual o filamento de RNA passa para que uma proteína seja sintetizada. Esse processo envolve, além do mRNA, o qual contém a seqüência de informações a serem traduzidas, entre sinais de inicio e fim e as seqüências correspondentes a cada aminoácido, o rRNA, o tRNA e mais algumas enzimas, tudo isso formando um complexo macromolecular. Essencialmente todo o processamento acontece em partículas chamadas de ribossomos. Estas partículas são compostas de algumas moléculas de RNA, enzimas utilizadas para atuar na formação das ligações peptídicas entre os aminoácidos, um sítio para depositar a molécula de mRNA, a qual será traduzida, e sítios para posicionamento e alinhamento

dos aminoácidos, carregados por tRNAs, os quais irão compor a proteína. Sendo um complexo, o ribossomo é a união de duas subunidades, cada qual se unindo no início da tradução. Uma vez que ribossomo é formado, tendo o mRNA presente no seu local específico, tRNAs trazem as moléculas de aminoácido para que elas sejam unidas. Nesse ponto é necessário ressaltar que o processo de decodificação do mRNA ocorre de forma que, como o mRNA é composto por nucleotídeos, existe um sistema de leitura que toma uma trinca de nucleotídeos do mRNA, chamada de códon, e os liga com uma trinca dos nucleotídeos presentes no tRNA, o qual transporta o aminoácido. Cada trinca do mRNA é chamada de códon e a trinca do tRNA é conhecida por anti-códon. Dando início a fase de iniciação da tradução o ribossomo prende-se ao mRNA e um primeiro tRNA trás consigo uma molécula particular, conhecida como tRNAfMet. Como o anti-códon presente no tRNA das duas é o mesmo, ambas podem reconhecer o códon de iniciação, porém apenas a tRNAfMet é utilizado para esse fim. Após esse procedimento inicial, entra em ação a fase de alongamento. Quando o tRNAfMet se liga ao mRNA ele ocupa o primeiro sítio livre do ribossomo, deixando um outro sítio disponível. Dessa forma um segundo tRNA ocupa o segundo sítio, desde que ele tenha o anti-códon que seja complementar ao códon apresentado. Uma vez que os dois sítios estão preenchidos é criada uma ligação peptídica entre os dois aminoácidos presentes nas extremidades do tRNAs, o tRNA, o qual trazia a tRNAfMet, se desprende e o ribossomo move-se para o próximo códon. Nesse ponto é importante lembrar que o movimento realizado pelo ribossomo é no sentido 5' 3'. Esse processo se dá até que um códon de sinalização de final de cadeia é atingido. Como não existe tRNA capaz de fazer correspondência ao códon o processo de alongamento para, dando início a fase de término. Uma vez que o processamento parou proteínas conhecidas como fatores de liberação, responsáveis pelo desprendimento da proteína criada do ribossomo, entram em ação. A Figura 8 exemplifica o processo de Tradução.

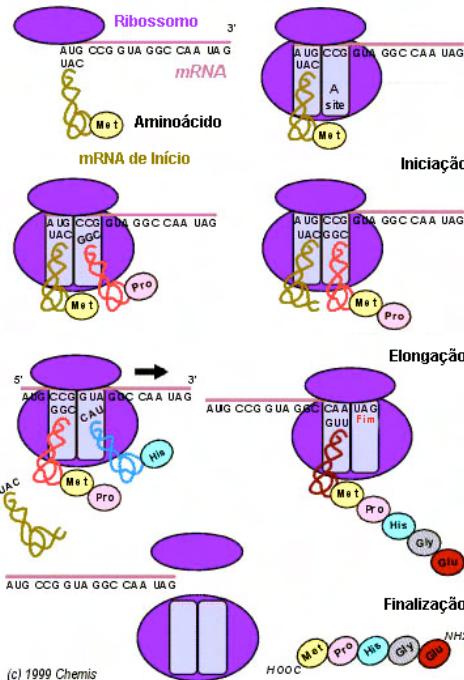


Figura 3 Representação gráfica do processo de Tradução.

Fonte: <<http://library.thinkquest.org/C0123260/basic%20knowledge/images/basic%20knowledge/RNA/translation%20steps.jpg>> Último acesso: 28 nov. 2008

3. Circuitos Gênicos

Circuitos gênicos são baseados na expressão gênica de uma faixa de DNA, ou seja, como apresentado no capítulo anterior, uma porção do DNA é transcrita para uma molécula de mRNA e esta, posteriormente, será traduzida em uma proteína (WEISS, 2001).

Partindo dessa característica e tomando o ponto de vista da Engenharia Elétrica pode-se observar que processos de inibir ou ativar um dado sistema de síntese podem ser vistos como uma chave liga/desliga para os processos. Outra relação existente entre os componentes celulares e os componentes eletrônicos que se faz necessária explicitar é a entrada de dados. Ambos trabalham com valores binários, sendo o valor zero definido pela ausência de tensão, no caso elétrico, ou ausência de uma concentração de uma proteína específica no meio celular; e o valor um definido pela presença de tensão ou presença da proteína no ambiente celular.

3.1. Inversor

Segundo Weiss (2001) A porta lógica mais básica é o inversor. Nele um sinal de valor binário zero será convertido para um sinal de valor um e vice-versa. O processamento desta porta se dá da seguinte forma: dada uma região do DNA para ser expressa, se for fornecida como entrada uma concentração de mRNA, o qual possui codificado em sua cadeia uma proteína repressora capaz de bloquear a transcrição do DNA, o mRNA esperado como saída do processo executado sobre a cadeia de DNA não será encontrado no meio, ou seja, dada uma entrada um o sistema produziu uma saída zero. Alternativamente, não sendo fornecido nenhum mRNA capaz de bloquear a transcrição do DNA dado o processo de transcrição poderá ocorrer livremente e o mRNA esperado aparecerá como saída da transcrição do DNA, ou seja, dada uma entrada zero o sistema produz uma saída um. Em linhas gerais, é dessa forma que um inversor funciona, porém existe todo um tratamento das informações que foi omitido. Esse tratamento corresponde a margem de ruído aceita, a restauração do sinal e uma interface padronizada para que este sistema possa compor outros mais complexos.

3.2. Porta Lógica AND

De maneira alternativa, Weiss (2001) argumenta que a porta AND trabalha com a recepção de sinais externos à célula, ou seja, ela é responsável por permitir que a célula, a qual possui essa implementação, identifique sinais recebidos de outras células. Como na porta anterior, a porta AND também apresenta as três fases de processamento do sinal de entrada e é composta por um ativador, um indutor e um gene a ser transcrito. O ativador e o indutor são responsáveis por tornar a transcrição possível uma vez que a RNA polimerase apresenta pouca afinidade pelo promotor ao qual ela deve se ligar. Sendo assim, se o circuito não receber como entrada o indutor nem o ativador, o valor de saída será baixo. Caso seja dado como entrada o ativador, mas não o indutor, também será gerado um baixo valor de saída. Na última configuração válida, tendo os dois componentes presentes na entrada do circuito, o indutor conectar-se-á ao ativador mudando sua forma, permitindo que esse complexo se une ao operador. Com o complexo unido ao operador a RNA polimerase conseguirá ligar-se ao gene, uma vez que a função do ativador é facilitar a união do complexo ribossômico ao material genético. O resultado disso será um valor alto na saída.

4. Modelagem De Um Circuito Meia-Soma Via Circuitos Gênicos

O grande desafio de se implementar circuitos digitais em sistemas bioquímicos está na conversão entre os paradigmas. Para que esse procedimento seja realizado com sucesso é necessário construir um modelo bioquímico e testá-lo para verificar se os resultados gerados por ele são coerentes com os esperados, ou seja, se o processamento na célula atinge os mesmos resultados que o processamento em cilício.

Inicialmente precisa-se definir qual circuito será codificado. Em seguida é necessário fazer um estudo de seus componentes básicos e, após isso, construir os modelos de cada componente. Por fim basta ligar os sub-componentes na ordem e quantidade necessária para então rodar testes, os quais verifiquem a aceitabilidade do modelo. Dessa forma, o circuito escolhido foi o circuito de meia-soma. Ele é composto por duas portas lógicas NOT e três portas lógicas AND, sendo que duas das portas AND juntamente com as duas portas NOT são combinadas para formar uma porta lógica XOR. A combinação da porta XOR com a porta AND restante gera o circuito de meia-soma.

Para a construção dos modelos é necessário escolher uma ferramenta capaz de simular as reações anteriormente descritas. No caso deste trabalho foi escolhido o software CellDesigner.

4.1. Inversor ou Porta Lógica NOT

O inversor é uma porta lógica que implementa a negação lógica. Sua característica principal é a de funcionar como um inversor de sinal, ou seja, a presença de um sinal A na entrada da porta, gera uma saída não-A, e vice-versa (TOCCI; WIDMER, 2003).

O modelo bioquímico gerado na ferramenta CellDesigner é representado na Figura 9. Para a existência de uma concentração de entrada A o gene Pz terá sua transcrição inibida por essa entrada, o que acarreta na não produção do mRNA₀, que seria a saída do sistema. No outro caso, quando a entrada A não está presente no sistema, Pz pode transcrever livremente gerando a saída mRNA₀.

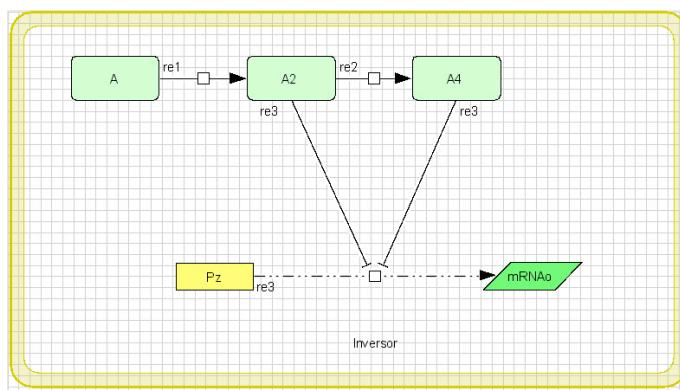


Figura 9 Modelo bioquímico da porta lógica NOT criado no programa CellDesigner.

4.2. Porta Lógica AND

A porta AND é uma porta lógica que implementa a conjunção lógica, ou seja, ela recebe dois sinais, A e B, de entrada e retorna como saída “verdadeiro” caso A e B estejam presentes ao mesmo tempo ou “falso” em qualquer um dos casos restantes. (TOCCI; WIDMER, 2003).

O modelo bioquímico gerado na ferramenta CellDesigner é representado na Figura 10. Nele é possível ver a utilização de duas proteínas (Ativador e indutor) como entradas do sistema e uma reação auxiliar, a transcrição de mRNA em resp, para gerar uma saída. As duas entradas, caso presentes no sistema, formam um complexo (AtivInd) o qual atua na ativação do mRNA, gerando o mRNAAtiv, e este será o passo final sendo traduzido na proteína de saída (resp). Sem a presença de qualquer uma elas, o complexo não é formado e não haverá a produção da proteína de saída.

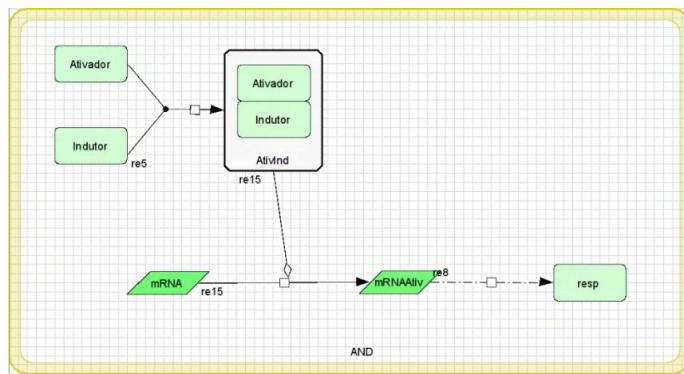


Figura 10 Modelo bioquímico da porta lógica AND criado no programa CellDesigner.

4.3. Porta Lógica XOR

Como foi citado anteriormente, a porta lógica XOR, também chamada de EXCLUSIVE OR, é formada a partir da composição entre as portas NOT, AND e OR. (TOCCI; WIDMER, 2003).

O modelo bioquímico gerado na ferramenta CellDesigner é representado na Figura 11. Nele é possível observar as duas entradas (Entrada_A e Entrada_B) sendo utilizadas em quatro módulos. Os dois primeiros são duas portas NOT sendo que cada uma delas gera a negação de cada uma das entradas. Os outros dois módulos são portas AND. O método do “Wire-OR” gera a saída final (XOR_AB). Caso as entradas estejam ausentes o circuito não produz resposta. Se apenas uma delas estiver presente, uma será produzida uma concentração de resposta com a mesma quantidade que a concentração da proteína inicial. Caso as duas entradas estejam presentes ocorrerá um “overflow” na produção de proteína de resposta, ou seja, será produzido mais do que a concentração necessária para se entender como um sinal de valor um, logo a interpretação dada a essa resposta é uma resposta de valor zero.

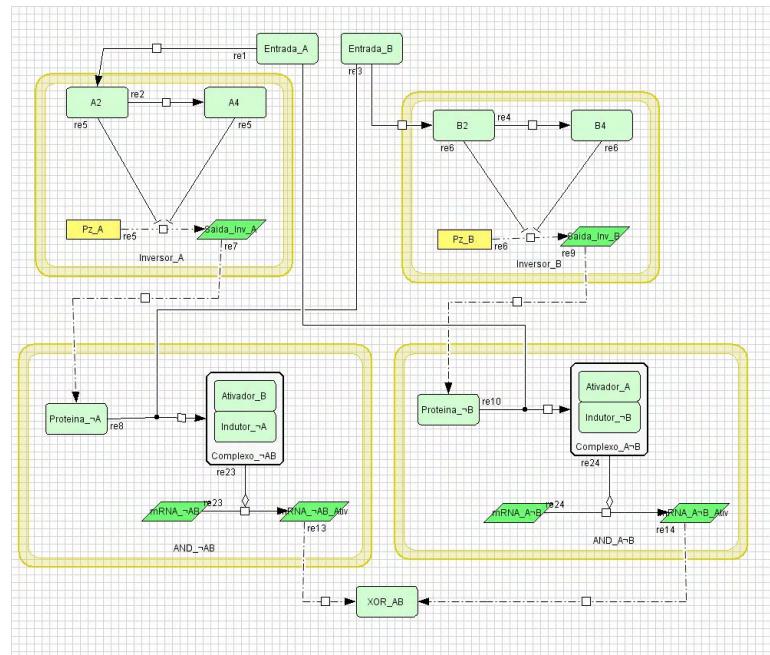


Figura 11 Modelo bioquímico da porta lógica XOR criado no programa CellDesigner.

4.4. Circuito Meia-Soma

Para este trabalho foi escolhido o circuito de meia-soma. Da definição da Eletrônica, um somador é um circuito digital responsável por fazer a adição entre números. Em especial, o circuito de meia-soma tem por função realizar a adição entre dois dígitos binários (A e B). Esse circuito produz, como resultado, uma soma (S) e um carry (C), ambos em valores binários. A soma é implementada através da porta lógica XOR e o carry é calculado através de uma porta lógica AND (TOCCI; WIDMER, 2003).

O modelo bioquímico gerado na ferramenta CellDesigner é representado na Figura 12. Nele é possível observar as duas entradas (Entrada_A e Entrada_B) sendo utilizadas em um XOR e em um AND bioquímicos. Caso não haja presença de nenhuma das duas entradas não haverá produção de nenhuma das duas saídas (XOR_AB e VaiUm). No caso de existir apenas uma das duas entradas o XOR apresenta uma saída com concentração suficiente para ser interpretada como um sinal um e o AND continua não apresentando concentração de saída, ou sinal de valor zero. No caso da presença das duas entradas, ocorre o “overflow” no XOR e seu resultado é interpretado como zero, porém o AND produz resposta dessa vez e o valor da concentração de sua proteína de saída pode ser interpretado como um sinal um.

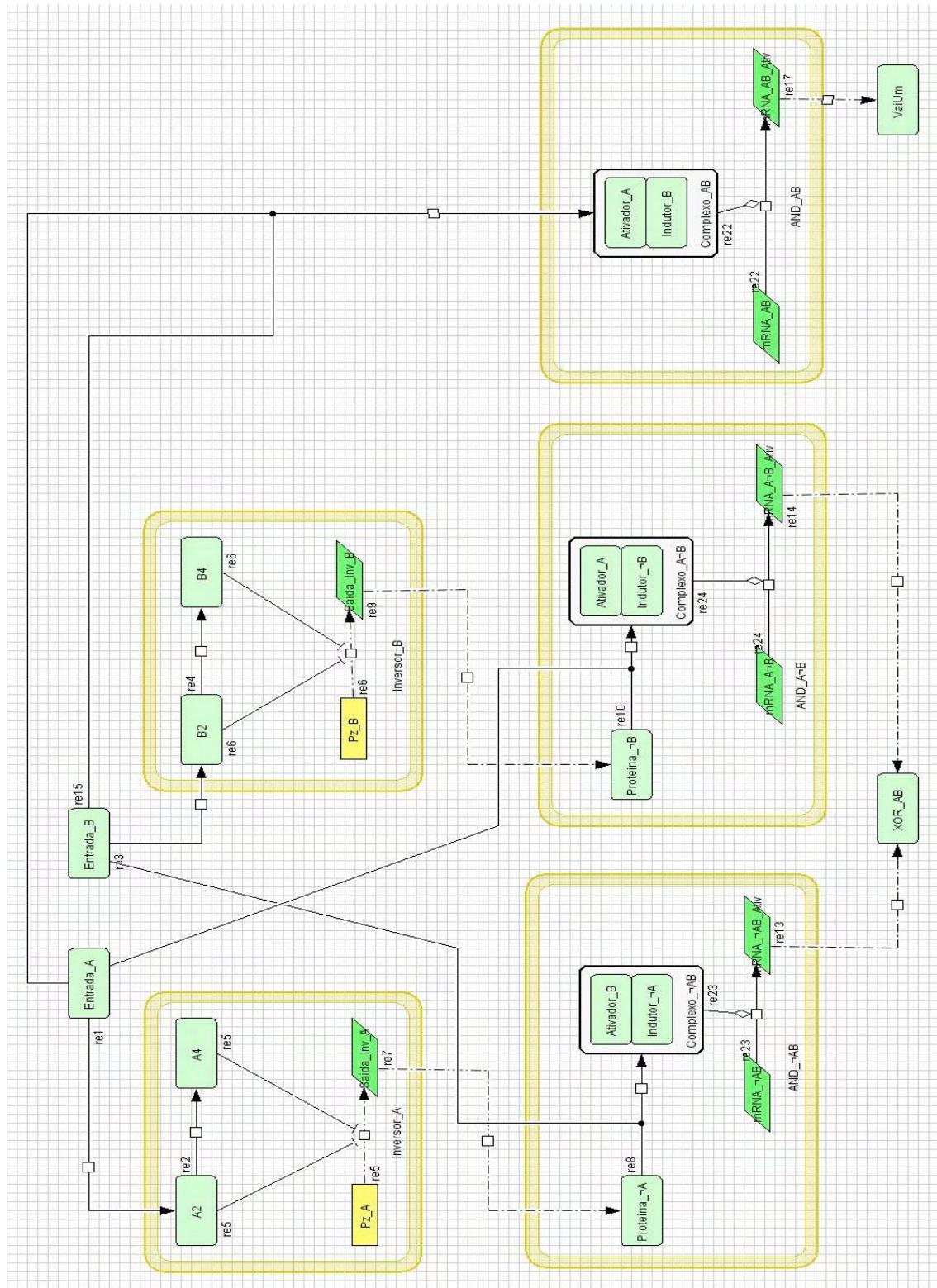


Figura 4 Modelo bioquímico do Circuito de Meia-Soma criado no programa CellDesigner. É de fácil visualização a presença da porta lógica XOR, circuito contendo os dois inversores e os dois ANDs, e uma porta lógica AND mais em cima para calcular o “carry” da soma.

Sistemas Biológicos apresentam uma grande dificuldade de se trabalhar devido ao fato de suas condições de funcionamento serem extremamente precisas, porém o ambiente aonde eles se encontram imersos apresenta uma quantidade de ruidos enorme para uma tentativa convencional de fazê-los funcionar da forma desejada. Com o avanço de áreas como Bioengenharia e Bioinformática, no entanto, foi possível estabelecer uma relação entre os mecanismos bioquímicos e as ferramentas de controle digital existentes na Engenharia Elétrica. Já existem trabalhos nos quais são propostas implementações das portas lógicas digitais mais básicas em meios bioquímicos e de forma funcional.

5. Conclusão e Trabalhos Futuros

O presente trabalho teve como objetivo, então, dar um passo a frente, utilizando essas novas ferramentas para desenvolver o modelo de um Biocircuito de Meia-Soma. Para isso foi necessário descrever as unidades básicas de processamento genético e os mecanismos responsáveis por esse processamento. Após apresentar o maquinário bioquímico foram desenvolvidos modelos conceituais matemáticos das portas lógicas digitais utilizando esses dispositivos bioquímicos. Uma vez que a base matemática foi introduzida, esses conceitos foram colocados em prática, através do software CellDesigner, para criar os modelos gráficos responsáveis pela demonstração do experimento. Foram criadas as portas lógicas NOT, AND, e XOR e, da união de uma porta XOR com uma porta AND, criou-se o Biocircuito de Meia-Soma.

A possibilidade de se implementar alguns circuitos de forma biomolecular apresenta algumas vantagens em relação aos componentes de silício uma vez que os dispositivos bioquímicos são da ordem de poucos nanômetros, ao contrário das implementações em silício, as quais ainda se encontram na casa das dezenas de nanômetros. Além disso, eles criam a possibilidade de se construir mecanismos regulatórios baseados em operações lógicas conhecidas, o que gera um controle das operações muito maior do que o que é fornecido pelas técnicas atualmente utilizadas.

No entanto existem limitações físicas para a criação de sistemas bioquímicos muito complexos, porque pra expandir esses sistemas em algum ponto fica inviável fornecer a quantidade de material genético necessário. Também existe uma grande variação entre o tempo de resposta de cada tipo de reação intra e intercelular, onde as reações de união entre moléculas pra formar os complexos e as ativações de RNAs e DNAs é da ordem de milisegundos enquanto que pra sentir uma variação de 50% na concentração da proteína que está sendo traduzida é da ordem de 1 hora, sendo que esses dados são válidos apenas para organismos unicelulares como a E. Coli (ALON, 2007).

A partir deste ponto pode-se então pensar em trabalhar as informações contidas neste trabalho com o intuito de expandir a gama de circuitos bioquímicos disponíveis para as outras operações aritméticas e também procurar novas reações bioquímicas, assim como outros métodos de modelagem e construção desses sistemas, como os motif de redes de transcrição apresentados por Alon (2007), para obter um aumento na velocidade das operações.

Referências Bibliográficas

ALON, U.(2007) An Introduction to Systems Biology. Chapman & Hall, Boca Raton, FL.

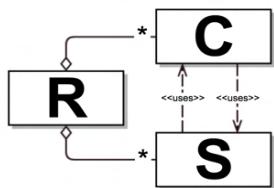
HUNTER, L. (2008) Molecular Biology for Computer Scientists. Disponível em: <<http://www.aaai.org/AITopics/classic/Hunter/01-Hunter.pdf>>. Último acesso: 28 nov. 2008.

MALACINSKI, G. M. (2005) Fundamentos de Biologia Molecular. 4. ed. Guanabara Koogan, Rio de Janeiro, RJ.

TOCCI, R. J.; WIDMER, N. S. (2003) Sistemas Digitais: Princípios e Aplicações. 2003. Prentice Hall Brasil, São Paulo, SP.

VOET, D.; VOET, J.G. (2004) Biochemistry. 3. ed.. Wiley, Hoboken, NJ.

WEISS, R. (2001) Cellular Computation and Communication Using Engineered Genetic Regulatory Networks. Tese (Ph.D.) - Massachusetts Institute of Technology, 2001. Disponível em <<http://www.princeton.edu/~rweiss/papers/rweiss-phd-thesis.pdf>>. Último acesso: 28 nov. 2008.



Proposta de Website de Dança de Salão baseada na Arquitetura e Usabilidade de Interfaces associada a Marketing Digital e Programação Visual

Raissa Gil Mattos¹, Pollyana Notargiacomo Mustaro^{1,2}

¹Faculdade de Computação e Informática (FCI) – Universidade Presbiteriana Mackenzie (UPM)

²Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) – Universidade Presbiteriana Mackenzie (UPM)

Consolação, 930 – 01.302-090 – São Paulo – SP – Brazil

raimagil@gmail.com, pollyana.mustaro@mackenzie.br

Abstract. *Currently, when it is desired to find information concerning ballroom dancing in Brazil, it is necessary to go through a number of different websites, something that takes a long time and knowledge in the matter to find what it is been search. From this, the research done, by means of the element of information architecture and usability guidelines, associated to digital marketing, proposes, with the use of wireframes, the development of a website focus exclusively for ballroom dancing. The use of visual programming concepts to the wireframes created made it possible the creation of an organized and harmonious website. Moreover, can be stand out that the concepts of marketing contributed for the making of a more attractive brand and a broader identification to merging her to the website, reinforcing it.*

Resumo. *Atualmente, quando se deseja encontrar informações sobre dança de salão no Brasil, é necessário consultar diferentes websites, o que requer maior tempo de busca e conhecimento de assuntos correlatos para que seja possível encontrar o que se deseja. A partir disso, a presente pesquisa, por meio do uso de elemento de arquitetura da informação e diretrizes de usabilidade, associadas ao marketing digital, propôs, por meio de wireframes, o desenvolvimento de um website voltado exclusivamente para dança de salão. O acréscimo dos conceitos de programação visual aos wireframes criados possibilitou a criação do website organizado e harmonioso. Além disso, destaca-se que os conceitos de marketing contribuíram para a elaboração e criação de uma marca mais atrativa e de identificação intuitiva para agregá-la ao website, fortalecendo-o.*

1. Introdução

Desde o início da história, a dança integra a vida do ser humano, estando associada à religião, às tribos e às culturas. Um dos tipos de dança é a dança de salão, caracterizada por ser um conjunto de ritmos e danças executadas em casais de forma harmônica [Volp

et al. 1995]. Destaca-se que a dança de salão auxilia na melhoria da qualidade de vida, pois contribui psicologicamente (expressa sentimentos e emoções), neurologicamente (envolve ritmo, sincronia e coordenação do corpo), fisicamente (caracteriza como um esforço físico em atividade conjunta ao ritmo) e socialmente (por promover encontros de dança e maior contato entre os integrantes) [Fonseca 2008]. Desta forma, a dança de salão também é uma forma de expressar sentimentos e emoções.

Contudo, há uma carência de propostas de centralização de informações sobre dança de salão num website brasileiro, ou mesmo que concentrem seus eventos e facilitem a busca de escolas destinadas a essa modalidade [Silla Jr. et al. 2007]. Neste sentido, o uso de estratégias de usabilidade associadas à arquitetura da informação, programação visual e conceitos pertinentes ao marketing digital pode permitir às pessoas que não estão familiarizadas à dança de salão encontrarem informações relacionadas a esse tipo específico de dança.

Tal desafio constituiu, então, o ponto de partida da presente pesquisa, sendo que se buscou desenvolver uma interface intuitiva e com usabilidade adequada a partir da montagem de esboços de páginas e de testes com futuros utilizadores. Tais esboços buscam, portanto, garantir uma interação e compreensão adequada do usuário com o sistema final, sendo feitos por meio de modelos de prototipação. Dentre eles destaca-se a prototipação em papel, que tem a vantagem de ser uma maneira simples e rápida de montar os modelos de página, além de facilitar a edição, já que na etapa de teste, as modificações são constantes [Silva et al. 2005]. Após a compreensão da proposta, se constroem *wireframes* para estruturar a visão do projeto, propiciando a realização de testes por usuários [Memória 2005].

A prototipação, usabilidade e arquitetura de software permitem o sucesso para um desenvolvimento de qualidade de um website, porém não basta apenas ele ser desenvolvido e implementado; é preciso a sua divulgação, de modo eficiente e eficaz, para isso é necessário o conhecimento dos conceitos de marketing, especialmente do marketing digital [Limeira 2003].

A partir disso, o objetivo desse trabalho foi desenvolver um website que centralizasse informações de dança de salão e permitisse a realização de buscas de maneira intuitiva. Isto exigiu uma coleta e organização de dados pertinentes aos aspectos apresentados e a aplicação de conceitos de marketing digital para estabelecer um mecanismo de interação com o usuário e tornar a proposta mais dinâmica para que a mesma seja acessada frequentemente e divulgada pelos próprios usuários.

O presente artigo encontra-se organizado da seguinte maneira: na seção 2 encontram-se os trabalhos relacionados à dança de salão, usabilidade de interfaces, arquitetura da informação, marketing digital e programação visual; a seção 3 aborda a metodologia da pesquisa, detalhando os métodos usados (questionários, *card sorting*, prototipação e os *wireframes*); a seção 4 mostra a análise dos resultados obtidos; a seção 5 agrupa a criação dos *wireframes* e o projeto do website; finalmente, a última seção aborda as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

2.1. Dança

A Dança de Salão, exemplo de Dança Social, constitui um conjunto de ritmos e danças executadas por casais (tanto na posição aberta como na posição fechada). Esses casais devem dançar e apresentar harmonia dos pares com a música e com o tempo relacionado ao movimento. Além de ser um meio para a socialização, a dança de salão não possui nenhuma restrição, sendo acessível a todo o tipo de público [Fonseca 2008].

O público-alvo inserido na dança de salão sempre busca comunicação e interação tanto com pessoas, como também na mídia. Por isso, ao criar um website com o intuito de atrair um público específico, torna-se relevante atentar não só para a satisfação deste como para a facilidade da navegação. Isso requer um investimento na arquitetura da informação para que se conheça o usuário e suas necessidades.

2.2. Usabilidade de Interface e arquitetura da informação

A interface constitui um elemento indispensável quando se trata de um website, ela facilita a interação do usuário com os dispositivos digitais, assim como a usabilidade. Segundo a ISO 9241-11, a usabilidade é definida como “medida na qual um produto pode ser usado por usuários específicos para alcançar objetivos específicos com eficácia, eficiência e satisfação em um contexto específico de uso”.

A utilização da usabilidade traz resultados positivos, como redução do tempo de acesso à informação, disponibilidade das informações, diminuição de erros, satisfação do usuário ao encontrar a informação procurada e a facilidade do usuário na percepção do website [Winckler e Pimenta 2002]. Contudo, a falta da usabilidade ocasiona diversos fatores negativos, como fadiga visual, stress, ansiedade, aborrecimentos e frustrações [Cybis et al. 2010]. Por isso, a identificação de problemas de usabilidade colabora para uma melhor solução ou redução desses erros, além da minimização do tempo, dos procedimentos de correção e dos custos de treinamento e manutenção [Martinez 2003].

Para um teste de usabilidade, a participação de cinco usuários é suficiente para encontrar os mesmos problemas que apareceriam com mais participantes, além de se obter um melhor custo-benefício. Porém há exceções, sendo que alguns estudos quantitativos requerem um número maior de usuários. Um exemplo disso é a classificação por cartão (*card sorting*), que requer pelo menos quinze usuários de teste [Nielsen 2012].

O *card sorting* é um método generativo com o objetivo de descobrir a visão das pessoas sobre determinados assuntos. Com esse método é possível perceber a distinção de pessoas, seus modos de pensar, analisar e agir. Por esse motivo devem-se coletar dados com um número razoável o bastante de usuários, pois quanto mais pessoas para analisar, mais pontos diferentes aparecerão, possibilitando a análise desses pontos para posteriormente acomodar as diferenças dos usuários da melhor maneira. Como o *card sorting* é um método de avaliação, o mais importante é ouvir os comentários dos usuários, buscando argumentos e justificativas para a forma com que eles ordenaram e agruparam os cartões. Essas justificativas e argumentos oferecem uma visão mais profunda dos modelos mentais dos usuários, o que é mais importante do que a mera

divisão e ordenação dos cartões. Para descobrir esses modelos mentais devem-se escrever os nomes e descrição dos itens nos cartões e pedir para cada usuário classificá-los e relacioná-los, dividindo-os em pilhas. O usuário poderá dividir em quantas pilhas ele achar necessário, caso hajam muitos cartões em um mesmo grupo pode-se pedir para dividir essa pilha em subgrupo. Além disso, é recomendável também solicitar ao usuário nomear as pilhas e também permiti-lo renomear alguns cartões se achar necessário, sempre buscando nomes que facilitem a compreensão e sejam autoexplicativos [Nielsen 2004].

Para obter-se um sistema interativo e comprehensível não é necessário apenas a usabilidade por testes de *card sorting*, os modelos de prototipação também são importantes para garantir que o sistema satisfaça o cliente [Silva et al. 2005]. Protótipo é um modelo real usado para simular ações de um sistema, com o objetivo de encontrar, por meio de testes e avaliações, necessidades ainda não observadas, erros não encontrados e confirmações de requisitos [Matheus Jr. 1998]. Há uma sutil diferença entre “modelo” e “protótipo”, o “modelo” é uma representação em escala menor, objeto a ser reproduzido por imitação, já o protótipo como falado antes, é um “modelo vivo”, que oferece a possibilidade de ver o funcionamento [Melendez Filho 1990].

O protótipo de papel é uma das técnicas mais rápidas e de baixo custo que permite um controle completo sobre como a interface comporta-se [Snyder 2001]. Dessa forma, colabora para testar ideias de design iniciais e corrigir problemas de usabilidade impedindo a implementação de um website que não funcione. Inclusive, as capturas de telas e/ou esboços das janelas são feitas à mão e permitem a simulação do comportamento do sistema, sendo que, por este motivo, as peças de interface devem ser manipuladas e os usuários devem ser orientados a tocar no papel, simulando um clique e escrever seus dados em campos de edição [Snyder 2003]. Com a prototipação em papel é possível evitar alguns problemas como conceitos e terminologia, navegação/fluxo de trabalho, conteúdo, *layout* da página e funcionalidade [Snyder 2001].

Tal processo é complementado pela arquitetura da informação, que trabalha com os processos cognitivos visando entender como as pessoas pensam, recordam, aprendem e como transformam informações em conhecimentos, instituindo uma visualização sistêmica que colabora para a organização de conteúdo facilitando, assim, a busca de informações [Toms 2002]. Inclusive, usuários possuem necessidades diferenciadas, o que exige conhecê-los com o intuito de suportar adequadamente o público específico ao qual se destina o sistema [Agner 2009], o que é feito por meio da organização, rotulação, navegação e busca. Essa abordagem é complementada pelo marketing (e mais especificamente pelo marketing digital), já que ele contribui para o conhecimento do usuário e possibilita o seu interesse em relação ao produto ou serviço oferecido.

2.3. Marketing e Marketing Digital

Pode-se dizer que o marketing objetiva criar valor para o cliente, resultando em vantagem competitiva para a empresa a partir de quatro parâmetros: produto, preço, promoção e ponto de distribuição [Limeira 2003]. Inclusive, uma das formas de se obter sucesso no marketing é o trabalho com a marca, pois esta possibilita associações, atribuições e personalidade da empresa permitindo que o produto tenha um valor significativo no mercado a partir dos fatores que propiciam o reconhecimento e

associação em diversas instâncias por meio de slogan, cores, símbolos, etc. [Kotler 2009].

Com a facilidade e agilidade no acesso às informações que a Internet proporcionou, muitas empresas passaram a utilizar o marketing digital [Morita 2010] para desenvolver os quatro espaços virtuais da atividade de marketing: informação (em que divulga e coleta informações necessárias), comunicação (em que se estabelecem os relacionamentos, comunicações e interações), distribuição (em que ocorre a entrega digital, eletrônica ou física de produtos e serviços) e transação (em que há negociações e fechamento de vendas) [Limeira 2003].

Inclusive, este contexto mudou completamente a dinâmica do mercado e do marketing, enquanto antes a comunicação ocorria de um-para-muitos, hoje ocorre de muitos-para-muitos. Atualmente o consumidor está no centro das ações, enquanto antes no marketing tradicional as ações ocorriam da empresa para o consumidor, hoje, é o consumidor que toma a iniciativa, é ele que busca a empresa e o produto, o que institui o que se denomina de inversão do vetor de marketing. Por isso, uma das formas do público-alvo relacionar-se com a marca ou produto é por meio da presença digital, ou seja, por meio de um website, banners distribuídos na rede ou de anúncios em displays digitais [Gabriel 2011].

3. Metodologia

A partir dos pressupostos, conceitos e dos objetivos da presente pesquisa, foi realizada uma investigação por meio de uma pesquisa de campo. Esta utilizou de um questionário [Fachin 2003] com pessoas de idade, gênero, conhecimento e tempo de dança distintos. Realizar uma pesquisa para o público-alvo, levando em consideração os tipos de pessoas dentro desse meio foi relevante para ter o conhecimento a respeito das particularidades de cada um e para entender o que cada subgrupo procura e espera encontrar em um website.

A pesquisa foi realizada com quarenta e seis pessoas, entre 17 e 59 anos, podendo ser respondido de duas formas, online (mediante um formulário disponibilizado no *Google Docs*) e em papel para atender a todo o tipo de público. Sendo que o questionário foi estruturado em quatro partes pensando em facilitar a compreensão do usuário, são elas: informações pessoais, motivação inicial, panorama atual, dança de salão e a internet.

Após os dados serem coletados, passou-se à análise e interpretação dos mesmos.

4. Análise dos resultados

Num primeiro momento trabalhou-se com o perfil dos usuários. Havia um número equilibrado entre homens e mulheres sendo 78% alunos e 22% professores. Estes professores possuem uma idade inferior aos alunos, onde a maioria esta na faixa dos trinta e um e quarenta e cinco anos. Observou-se também que a experiência de uma pessoa está diretamente relacionada com o tempo que ela dança, e consequentemente com o fato de ser aluno ou professor. Assim, pessoas categorizadas como professores possuem mais experiência na dança, já que 70% dos professores e apenas 8% dos alunos estão a mais de quatorze anos estudando a dança de salão e 0% dos professores e

61% dos alunos estão a menos que sete anos. Já em relação à Internet foi observado que 56% dos entrevistados não acessam nenhum website sobre dança de salão.

Em suma, foi possível concluir que o interesse dos entrevistados pela dança surgiu pela própria dança e por influência de amigos que já praticavam a dança. Já para a escolha de uma escola de dança de salão, as opções de horários oferecidos pela escola juntamente com a sua localização são os fatores mais determinantes. Para um website, interessaria, portanto, aos entrevistados uma agenda de eventos, como também vídeos de coreografias e novidades sobre a dança de salão. O fator mais importante para a escolha de um evento, segundo 25% são os frequentadores do baile. Enquanto, para descrever um evento, os entrevistados acham mais relevantes informações como: dados gerais (local, hora e data), quais ritmos e bandas/DJs tocarão, o valor de entrada (preço) e a descrição do lugar.

Como segunda abordagem de coleta de dados usou-se o *card sorting*. Esta foi realizada com 15 pessoas [Nielsen 2004], sendo que todas elas pertencem ao público-alvo do website (pessoas que praticam a dança de salão). Durante o teste foi possível perceber que os links e sublinks, de modo geral, estavam autoexplicativos. A maioria das pessoas conseguiu entender os conforme descrição sugerida enquanto os que não conseguiram, chegaram à ideia principal do link (Figura 1).

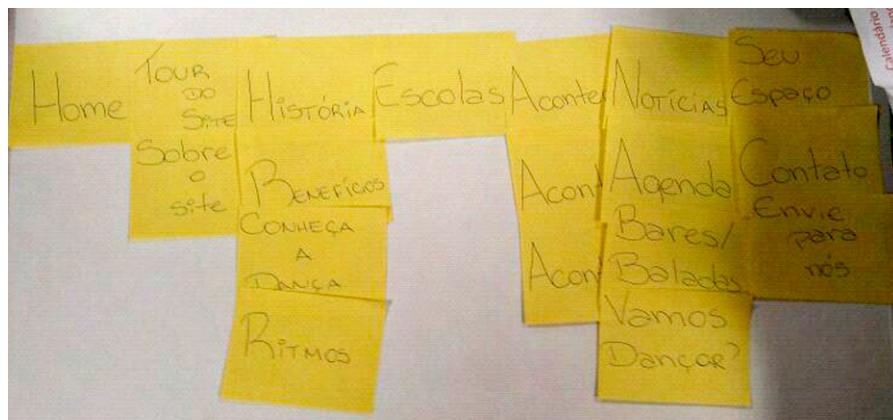


Figura 1. Teste de *card sorting*

Com essas informações foi possível tomar conhecimento a respeito dos interesses do público-alvo do website, assim como desenvolver o website.

Cabe também destacar que houve um link mais crítico, “Seu Espaço”, pois uma considerável parcela dos participantes do teste imaginou que se referia ao perfil do usuário (mediante login), sendo que uma pessoa sugeriu renomear o link para “Nosso Espaço” com o intuito de sugerir uma página colaborativa, onde o usuário contribuísse com o website enviando fotos, vídeos, comentários, etc. Essa ideia de renomear o link para “Nosso Espaço” foi levada a algumas pessoas, resultando em uma ideia de ser um espaço para um grupo de pessoas interagir, discutir, comentar, tirar dúvidas e fazer sugestões e reclamações. Como o link “Nosso Espaço” também não atingiu a ideia proposta, foi levada a algumas pessoas a mudança desse link para “Espaço Interativo”. Os resultados foram melhores do que as duas primeiras opções ao transmitir a proposta de página conectada com redes sociais – em forma de mural – possibilitando deixar

recados ou comentários, enviar vídeos, bem como convidar pessoas para algum evento. Outro sublink que precisou ser renomeado foi “Tour do site” por “Mapa do site”, já que 40% das pessoas não compreenderam a metáfora empregada.

Todas as observações adquiridas por meio do teste de *card sorting* foram analisadas, de maneira que as modificações julgadas necessárias foram realizadas.

5. Proposta de website voltado ao público de dança de salão

Em seguida passou-se à protipação em papel, que envolveu a seleção de todas as tarefas possíveis para cada link e sublink e formulação das perguntas sem incluir comandos reais ou links de navegação [Nielsen 2009]. Depois as tarefas foram divididas entre cinco usuários [Nielsen 2012], de forma que eles não tivessem tarefas parecidas. Com a prototipação em papel foi possível encontrar, baseando-se nos itens levantados por Snyder (2001), alguns pontos a serem melhorados, como “conceitos e terminologia” e “navegação e fluxo de trabalho”.

Após realizados todos os testes e feitas todas as modificações necessárias, foram montados os *wireframes* – rascunhos de um website que permitem uma visão geral a respeito do fluxo de dados, navegação, agrupamento, ordem e hierarquia do conteúdo [Memória 2005] – (Figura 2) por meio do software Pidoco.

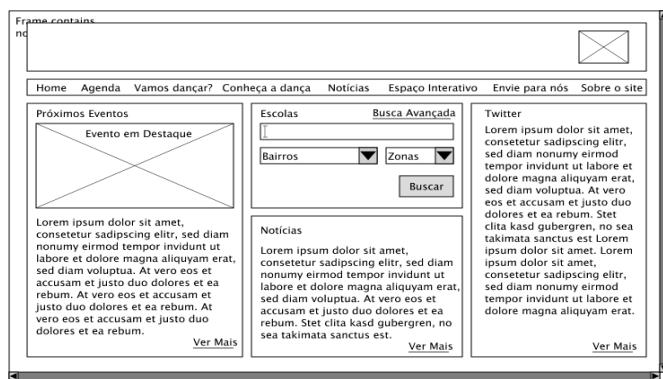


Figura 2. Wireframe da página inicial do website

Percebe-se que se procurou elaborar uma homepage que permitisse ao usuário ter uma visão geral da proposta e percorrer por todo o website [Siegel 1996], seja por meio do menu na homepage ou por meio dos elementos presentes na página inicial. Além disso, no corpo de texto da página principal são mostrados alguns conteúdos dos links, como um breve resumo, para atrair o usuário de forma que ele se interesse e queira permanecer mais tempo no website. Para atrair ainda mais o usuário, foi inserida na homepage a relação de eventos, conteúdo mais procurado pelos usuários, juntamente com uma imagem do evento em destaque, já que imagens tornam o website mais dinâmico, chamando a atenção do usuário. Além da relação de eventos foi definida uma área para a busca de escolas para que o usuário tenha o conhecimento que o website também possui opções para iniciantes, e não apenas para os já praticantes da dança de salão. Também foi previsto um espaço para notícias, contendo um link que direcionará para esta página, sendo este o de eventos previstos para atualização semanal para não tornar a proposta estática [Siegel 1996]. Já o Twitter (*microblogging*) tem como objetivo criar compromisso/fidelização por meio de conteúdo diário, bem como para a

instituição de interação dos usuários com o website em tempo real. Em seguida, passou-se ao estudo voltado à elaboração da marca, que deve ser traduzida por meio de um nome fácil de pronunciar, de reconhecer e de lembrar [Serralvo et al. 2008]. Na logomarca do website também foi utilizado um dos tipos básicos de denominação institucional, a “contração como palavras” [Perez 2004]. De forma que na logomarca aparece a sigla “BPQ”, referência às três primeiras letras do nome atribuído ao website (“Bota Pra Quebrar”), elaborado conforme os preceitos apresentados anteriormente.

Depois de criado o nome foi necessário criar uma identidade visual para que ela seja reconhecida rapidamente. No caso da logomarca do website “Bota Pra Quebrar”, logomarca mista [Heilbrunn 2004] que apresenta elementos linguísticos e icônicos, a mesma foi projetada para fazer analogia à dança de salão. Dessa forma, a sigla “BPQ” foi o elemento mais trabalhado, enquanto os outros dois constituíram um complemento à logomarca. Pois, com a sigla “BPQ” em letra minúscula foi possível dar um efeito de espelho já que o “b” é reflexo do “p” que por consequência é reflexo do “q”. Com o auxílio da imagem das duas pessoas dançando aumenta ainda mais a compreensão da logomarca.

Assim que a logomarca foi definida passou-se ao design da página do website, o qual buscou, do ponto de vista estético, ser adequadamente organizado e dimensionado. A disposição dos elementos foi pensada de forma a fazer sentido ao usuário para que seja mais intuitiva a sua navegação. Da mesma forma, trabalhou-se no sentido de obter equilíbrio e a harmonia do website por meio do posicionamento dos elementos pertencentes ao conteúdo da página [Dabner 2003], assim como pelas cores utilizadas [Farina 1994; Fraser 2007]. Cada cor possui uma associação, um simbolismo, causando reações diferentes em cada indivíduo. O violeta (nome genérico que se dá a todas as cores resultantes da junção do vermelho com o azul), geralmente, é facilmente memorizado e quando dessaturado com o branco (formando os lilases) produz tonalidades de intensa luminosidade e beleza [Farina 1994], o que é pertinente a um website de dança de salão. Com a definição do nome, da marca e das cores, juntamente com a proposta dos wireframes, foi possível montar o *layout* do website (Figura 3).

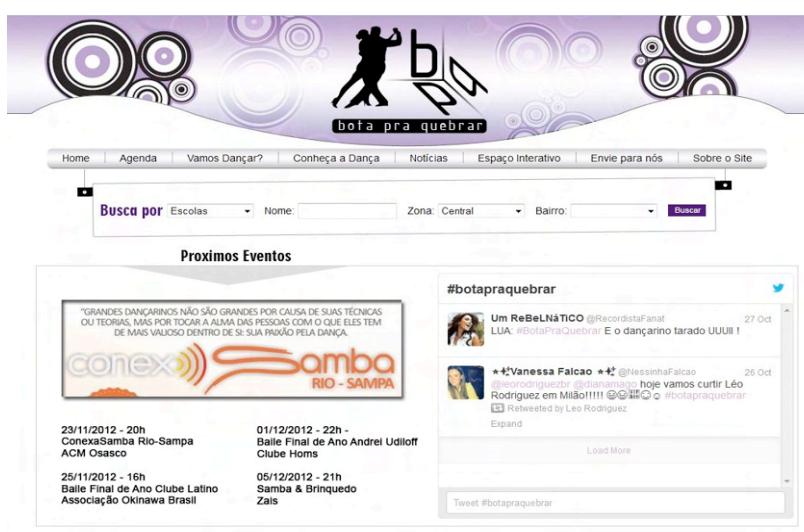


Figura 3. Layout da página inicial

Contudo, é possível perceber que foram implementadas algumas mudanças em relação à proposta inicial para evitar a sobrecarga informacional e ocasionar erros durante o uso [Toms 2002].

6. Conclusões e trabalhos futuros

No presente artigo foram apresentados subsídios teóricos que embasaram uma pesquisa de campo (envolvendo questionário, *card sorting*), bem como o desenvolvimento de uma proposta de website brasileiro voltado ao público-alvo de dança de salão.

Destaca-se, inclusive, que os instrumentos escolhidos foram fundamentais para obter uma visão dos modelos mentais dos usuários e descobrir quais elementos do design não funcionam conforme esperado para, então, modificá-los. De forma complementar, a prototipação em papel facilitou a interação com o público-alvo em seu ambiente de interação: escolas de dança de salão. A prototipação em papel colaborou, ainda, para a realização de testes de design iniciais e para corrigir problemas de usabilidade em relação à compreensão do usuário, assim como de ordenação e fluxo de dados, além de funcionalidades indesejadas ou faltantes. Encontrados os problemas, foi possível adequá-los para que os *wireframes* fossem montados, permitindo uma visão mais ampla do website (fluxos de dados, navegação, agrupamento, ordem e hierarquia do conteúdo), colaborando para uma análise final antes de o website ser construído e implementado.

Ainda antes da construção e implementação do website, foi elaborada sua marca e seu cabeçalho. Por fim, unindo todos os materiais até aqui colhidos, foi possível construir e implementar um website que possua uma usabilidade adequada e conteúdos necessários ao público brasileiro de dança de salão.

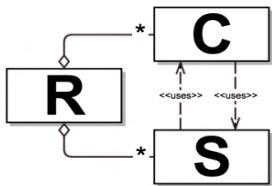
Como possíveis trabalhos futuros, pode-se apontar a aplicação de outros testes de usabilidade, como o *eye tracking*, além de trabalhar com conceitos de acessibilidade no website. Ainda podem-se acrescentar funcionalidades faltantes que foram propostas na pesquisa, além de novas funcionalidades, como inserir cadastros de usuários para que sejam possíveis anúncios e promoções no website e o estabelecimento de uma rede social interna, para aumentar o nível de interação no website.

Referências Bibliográficas

- Agner, L. (2009), Ergodesign e arquitetura de informação: trabalhando com o usuário, Quartet.
- Associação Brasileira de Normas Técnicas. NBR 9241-11. (2002). Requisitos ergonômicos para trabalho de escritório com computadores: Parte 11 – Orientação sobre usabilidade.
- Cybis, W., Betiol, A. H. e Faust, R. (2010), Ergonomia e Usabilidade: Conhecimentos, Métodos e Aplicações, Novatec.
- Dabner, D. (2003), Guia de artes gráficas: design e layout - princípios, decisões, projectos, Barcelona.
- Fachin, O. (2003), Fundamentos de metodologia, Saraiva.
- Farina, M. (1994), Psicodinâmica das cores em comunicação, Edgard Blücher, 4. ed.
- Fraser, T. (2007), O guia completo da cor, Ed. SENAC São Paulo.

- Fonseca, C. C. (2008) “Esquema Corporal, Imagem Corporal e Aspectos Motivacionais na Dança de Salão”. Programa de Pós-Graduação Stricto Sensu em Educação Física – Universidade São Judas Tadeu, São Paulo.
- Gabriel, M. C. C. (2011), Marketing na era digital: conceitos, plataformas e estratégias, Novatec.
- Heilbrunn, B. (2004), A logomarca/ Benoît Heilbrunn, UNISINOS.
- Kotler, P. (2009), Marketing para o século XXI: Como criar, conquistar e cominar mercados, Ediouro.
- Limeira, T. M. V. (2003), E-marketing: o marketing na internet com casos brasileiros, Saraiva, 2. ed. rev. atual.
- Martinez, M. L. (2003) “Um método de web design baseado em usabilidade”, In: V International Conference on Graphics Engineering for Arts and Design.
- Matheus Jr., D. (1998), Controle de qualidade de software prototipação, Dissertação de Mestrado, Universidade Presbiteriana Mackenzie.
- Melendez Filho, R. M. (1990), Prototipação de sistemas de informações: fundamentos, técnicas e metodologia, LTC – Livros Técnicos e Científicos.
- Memória, F. (2005), Design para a Internet – Projetando a experiência perfeita, Campus/Elsevier.
- Morita, M. Marketing digital. Curitiba, IESDE, 2010.
- Nielsen, J. (2004), “Card Sorting: How Many Users to Test”, <http://www.useit.com/alertbox/20040719.html>.
- _____. (2009), “Card Sorting: Pushing Users Beyond Terminology Matches”, <http://www.useit.com/alertbox/word-matching.html>.
- _____. (2012), “How Many Test Users in a Usability Study?”, <http://www.useit.com/alertbox/number-of-test-users.html>.
- Perez, C. (2004), Signos da marca: expressividade e sensorialidade, Thomson.
- Serralvo, F. A. (Org.). (2008), Gestão de marcas no contexto brasileiro, Saraiva.
- Siegel, D. (1996), Criando sites arrasadores na web: a arte da terceira geração em design de sites, Quark.
- Silla Jr., C. N., Kaestner, C. A. A. e Koerich, A. L. (2007), “The Latin Music Database: Uma Base de Dados Para a Classificação Automática de Gêneros Musicais”, In: Anais do 11 Simpósio Brasileiro de Computação Musical, SBC, pp. 167-174.
- Silva, A. C. et al. (2005), “Integrando Visões de IHC e de ES por Padrões no Desenvolvimento por Prototipação Descartável”, In: Proceedings of the 2005 Latin American conference on Human-computer interaction, pp. 223 – 234.
- Snyder, C. (2003) Paper prototyping. San Francisco.
- _____. (2001), “Paper prototyping: Sure, it's low-tech, but this usability testing method can help you sidestep problems before you write your code” <http://www.cim.mcgill.ca/~jer/courses/hci/ref/snyder.pdf>.
- Toms, E. G. (2002). Information Interaction: Providing a Framework for Information Architecture. In *Canada Journal of the American Society for Information Science And Technology*.
- Volp, C. M., Deutsch, S. e Schwartz, G. M. (1995). Por Que Dançar? Um Estudo Comparativo. In *Motriz*, Rio Claro, v.1, n.1.

Winckler, M A. e Pimenta, M. S. (2002), “Avaliação de Usabilidade de Sites Web”, In: Nedel, L. P. (Org.). Escola de Informática da SBC Sul (ERI 2002), Fortaleza, pp. 336-347.



RISCOS ADVINDOS DA UTILIZAÇÃO DE BIG DATA E COMPUTATIONAL SOCIAL SCIENCE

Vivaldo José Breternitz, Leandro Augusto da Silva, Fábio Silva Lopes

Faculdade de Computação e Informática, Universidade Presbiteriana Mackenzie

Consolação, 930 – 01.302-090 – São Paulo – SP – Brazil

vjbreternitz@mackenzie.br, leandro.augusto@mackenzie.br,
flopes@mackenzie.br

Abstract. The abundance of data and the speed at which they are generated have led to changes in planning and operation in various organizational instances. Big Data, the name given to a set of technology trends that allows a new approach to the treatment and exploration of large sets of data for decision making, allows the dynamics of a society can be analyzed from the perspective of information. Computational Social Science (CSS), as this type of analysis is defined, suggests a discussion of the risks in the discovery of information in this social context. It is in this discussion that the work fits, presenting Big Data and CSS, and discussing the risks inherent in its practical uses.

Resumo. A abundância de dados e a velocidade em que eles são gerados têm provocado mudanças de planejamento e operação em diversas instâncias organizacionais. Big Data, nome dado a um conjunto de tendências tecnológicas que permite uma nova abordagem para o tratamento e exploração de grandes conjuntos de dados para fins de tomada de decisões, permite que a dinâmica de uma sociedade possa ser analisada, sob a perspectiva da informação. Computational Social Science (CSS), como este tipo de análise é definida, sugere uma discussão sobre os riscos na descoberta de informações nesse contexto social. É nesta discussão que o trabalho se insere, apresentando Big Data e CSS, e também discutindo os riscos inerentes em seu uso prático.

1. Introdução

Quando uma nova tecnologia começa a emergir com força, as comunidades acadêmica e de negócios, seguidas pelo restante da sociedade, procuram conhecer os benefícios que a mesma pode trazer às pessoas e organizações. Apenas mais tarde, quando essa nova tecnologia já está sendo utilizada, os riscos decorrentes de seu uso começam a ser percebidos, partindo-se daí para a busca de soluções que possam mitigar esses riscos.

Big Data vive uma situação como a acima descrita: o entusiasmo despertado pelos benefícios que podem ser obtidos com seu uso está chegando às comunidades acadêmica e de negócios, mas quase nada vem sendo pensado em termos de riscos que podem ser trazidos pelo seu uso intensivo.

São exceções algumas considerações acerca de ameaças à privacidade: a revista *The Economist* [Economist, 2010] já mencionava o *trade-off* entre os potenciais ganhos econômicos trazidos pela utilização de Big Data e os riscos à privacidade. Tene e Polonetsky [2012] alertam para os riscos cada vez maiores e para a necessidade de aperfeiçoamento do marco legal relativo ao assunto; Rossouw [2012] relata propostas da Comissão Europeia (CE) no sentido de adequar a legislação da União Europeia a essa nova realidade; a CE considera, por exemplo, as normas de privacidade adotadas em março de 2012 pelo Google como "altamente arriscadas", ainda que não as tenha declarado ilegais. A visão da CE é de que unificar os dados de usuários de diferentes serviços representa risco severo para a privacidade individual.

Além dos aspectos ligados ao risco, a sociedade como um todo desconhece os conceitos básicos relativos ao Big Data.

2. Objetivos e aspectos metodológicos

Dado esse cenário, decidiu-se desenvolver este ensaio, que teve como objetivo apresentar os conceitos básicos relativos a Big Data e discutir alguns aspectos relevantes relativos aos riscos trazidos pela disseminação da utilização dessa ferramenta, especialmente aqueles ligados à Computational Social Science (CSS), de forma a gerar subsídios para os envolvidos com o tema.

Do ponto de vista metodológico, o ensaio foi produzido a partir de pesquisa de natureza exploratória, que conforme dizem Sellitz *et al* [2001], tem como objetivo proporcionar maior familiaridade com o problema, torná-lo mais explícito e construir hipóteses para posterior investigação.

A pesquisa exploratória somou-se a experiência profissional e acadêmica de seus autores, gerando o ensaio, que Ortega y Gasset [2004] define como “ciência sem prova explícita”, qualificando-o como um texto literário breve, que expõe ideias, críticas e reflexões a respeito de um dado tema, defendendo um ponto de vista pessoal e subjetivo sobre o mesmo sem se pautar por formalidades como documentos e provas empíricas ou dedutivas de caráter científico.

Passa-se agora a apresentar os conceitos básicos e a discutir aspectos relevantes relativos ao assunto, conforme os objetivos acima mencionados.

3. Apresentando Big Data e tecnologia a ele associada

Ainda não há uma definição precisa para Big Data, mas pode-se usar o termo para designar um conjunto de tendências tecnológicas que permite uma nova abordagem para o tratamento e exploração de grandes conjuntos de dados para fins de tomada de decisões.

Alguns autores, como Zikopoulos *et al* [2012] dizem que Big Data se caracteriza por quatro aspectos: volume, velocidade, variedade e veracidade.

O aspecto volume refere-se ao fato de que a quantidade de dados disponível em forma digital cresce de maneira exponencial, provenientes não só de sistemas convencionais, também de fontes como Facebook, Tweeter, You Tube, RFID, eletrônica embarcada, telefones celulares e assemelhados, sensores de diversos tipos etc.

Ao final de 2012, McAfee e Brynjolfsson [2012] estimavam que cerca de 2,5 *exabytes* de dados eram criados a cada dia, e que este número irá dobrar a cada 40 meses, aproximadamente. Os mesmos autores dizem que na atualidade a cada segundo, mais dados transitam pela internet do que o total armazenado na mesma há 20 anos. Apenas o Walmart coleta mais de 2,5 *petabytes* a cada hora, derivados das transações efetuadas por seus clientes.

McAfee e Brynjolfsson [2012] apresentam outro aspecto relevante de Big Data: a velocidade em que dados podem ser capturados e processados, quase em *real time*, podendo dar a uma organização vantagem competitiva. Exemplificam essa afirmação relatando experimento conduzido pelo grupo de pesquisa do Professor Alex Pentland, do MIT Media Lab: o grupo capturou dados relativos à localização de celulares de forma a inferir quantas pessoas colocaram seus carros nos estacionamentos de lojas do grupo americano Macy's no Black Friday de 2011 (data que marca o inicio da temporada de compras de Natal nos Estados Unidos); isso permitiu estimar com precisão as vendas dessas lojas antes mesmo que elas ocorressem, gerando vantagens competitivas que poderiam ser utilizadas por áreas comerciais, de *marketing* e por terceiros, como investidores em bolsas de valores.

No que se refere à variedade, cabe registrar que além de fontes diferentes, tais dados têm, frequentemente, características que fogem das tratadas pelos sistemas convencionais, não sendo estruturados e referindo-se a coisas como movimento, temperatura, umidade e até mesmo variações na composição química do ar (Lohr, 2012]. Neste aspecto, a internet das coisas (Internet of Things), é uma nova promessa de integração de várias tecnologias e soluções de comunicação, de modo a distribuir inteligência para diferentes dispositivos de modo a prover interação e cooperação entre eles (Atzori, Iera e Morabito, 2010]. No entanto, além da interação e cooperação, estes dispositivos também geram dados que podem ser armazenados, compartilhados, agregados e analisados.

O aspecto veracidade está relacionado ao fato de que os dados não são “perfeitos”, no sentido de que é preciso considerar o quanto bons devem ser os mesmos para que gerem informações úteis e também os custos para torná-los bons.

Alguns autores consideram um quinto aspecto, a validade dos dados, ou seja, sua vida útil, o tempo em que os mesmos precisam ser mantidos [Taube, 2012]. Esses aspectos são coletivamente chamados 4V ou 5V.

As ferramentas computacionais, por outro lado, vêm acompanhando o crescimento dessa velocidade e do volume de dados, em termos de capacidade de armazenamento e processamento. Destacam-se nesse assunto as pesquisas em corrente contínua de dados (*stream computing*) e em técnicas de inteligência artificial (*artificial intelligence*).

No modelo convencional de armazenamento de dados e tomada de decisão, a organização filtra dados dos seus vários sistemas e após criar um *data warehouse*, constrói consultas (*queries*) que subsidiarão a tomada de decisões. Na prática faz-

se garimpagem em uma base de dados estática, que não reflete o momento, mas sim o contexto de horas, dias ou mesmo semanas atrás. Com *stream computing*, esse *mining* ocorre em tempo real, com uma corrente contínua de dados (*streaming data*) atravessando um conjunto de *queries* - isso pode ser considerado um novo paradigma.

Na Inteligência Artificial, por sua vez, destacam-se os estudos em processamento de linguagem natural (*natural-language processing*), reconhecimento de padrões (*pattern recognition*) e aprendizado de máquina (*machine learning*) que podem ajudar a extrair dos grandes volumes de dados (estruturados ou não estruturados) conhecimento para auxiliar a tomada de decisões [Lohr, 2012].

Observa-se também a evolução relativa aos modelos de persistência de dados. O modelo hierárquico utilizado nos anos 1960 e 1970 foi substituído pelo modelo relacional nos anos 1980, e este se mantém em uso na grande maioria das aplicações em produção. Contudo, a nova geração de bancos de dados conhecidos como NoSQL, apresentam-se como novas opções mais eficientes para manipulação de grandes volumes de dados não estruturados, principalmente abordando pontos como estrutura não relacional, plataforma distribuída, código aberto e horizontalmente escaláveis [NoSQL, 2013].

Armazenar é apenas parte do negócio. A recuperação e análise dos dados têm ganho atenção no que diz respeito ao desenvolvimento de ferramentas que ampliam a capacidade analítica em grandes volumes de dados. Contudo, as ferramentas de *Business Intelligence* (BI), que tem esse objetivo, não trabalham em tempo real. Esta característica está atribuída às novas ferramentas denominadas *Business Analytics* (BA), conforme diz Gnatovich [2006].

As possibilidades de aplicação desses conceitos são inúmeras, em finanças, saúde segurança, manufatura etc. McAfee e Brynjolfsson [2012] conduziram estudos que levaram à conclusão de que as empresas que efetivamente utilizam Big Data são 5% mais produtivas e 6% mais lucrativas que seus competidores – na atualidade esses números são um poderoso argumento em prol da utilização dessa abordagem. Ben Waber, pesquisador do Instituto de Tecnologia de Massachusetts (MIT), afirma: “Se as pessoas aprenderam alguma coisa nas últimas décadas, foi que usar dados para construir organizações é melhor do que seguir instintos.” [Battibugli, 2013].

Moraes [2012] relata como a aplicação de Big Data ajudou na campanha de reeleição do presidente norte-americano, Barack Obama, permitindo orientar voluntários, indicar as melhores formas de arrecadar fundos e apontar quem poderia ser convencido a apoiar a reeleição do presidente; os responsáveis pela campanha deram prioridade ao uso de Big Data em detrimento da propaganda pela televisão.

Os responsáveis pela campanha usaram a Amazon Web Services para armazenar e processar o enorme volume de dados capturados. Foram adotadas ferramentas de computação em nuvem para lidar com bancos de dados, como o Amazon DynamoDB e Amazon RDS. Uma das principais preocupações foi permitir que a base de dados fosse trabalhada por diferentes aplicativos escritos em diversas linguagens de programação – para isso, se desenvolveu o Narwhal, um conjunto de serviços que funcionava como *interface* entre os dados e os muitos programas criados para a campanha.

4. Apresentando Computational Social Science (CSS)

Computational Social Science (CSS) pode ser definida como a ciência que comprehende a investigação da dinâmica social conduzida de forma interdisciplinar, sob a perspectiva da informação e por meio do uso de sistemas computacionais avançados [Cioffi-Revilla, 2010], como Big Data; a academia já começa a discutir sua aplicação em estudos ligados às ciências sociais, políticas públicas e comportamento de indivíduos e grupos [Global Pulse, 2012].

King [2013] descreve como estudantes de cursos ligados às ciências sociais, usualmente em nível de pós graduação, estão passando a receber treinamento formal em computação, como parte de sua formação para que possam atuar na área; este fenômeno vem se cristalizando com a criação em algumas universidades de departamentos ou cursos usualmente chamados “Computational Social Science” ou “Applied Computational Science”; na Harvard University foi criado o IQSS, Institute for Quantitative Social Sciences (<http://iq.harvard.edu>), com o objetivo de dar suporte à pesquisa na área.

Este novo campo de conhecimento é impulsionado pelos fatores anteriormente mencionados como capacidade computacional, ferramentas de apoio e o grande volume de dados gerado por diversos dispositivos e acumulados em diferentes repositórios.

5. A utilização de Computational Social Science - riscos

A capacidade, inerente a Big Data, de coletar e analisar grandes volumes de dados permite que se revele padrões referentes a indivíduos e grupos e que se simule o comportamento dos mesmos quando alteradas determinadas variáveis [Agarwal *et al*, 2008].

A sociedade como um todo deve preocupar-se com a utilização dessas capacidades, por empresas, governos e outros tipos de organização – empresas e governos são, na atualidade, os detentores de vastas quantidades de dados que podem ser utilizados para CSS.

O senso comum diz que o acesso a certos dados não deve ser permitido sem muitos cuidados; por essa razão existem leis que restringem a gravação de conversas telefônicas e o acesso a registros médicos, garantem a inviolabilidade da correspondência etc.

A gravidade dos danos gerados por acesso e uso indevidos é quase sempre óbvia. No entanto, a combinação de dados aparentemente inofensivos provenientes de diversas bases ou a análise de grandes bases de dados pode gerar informações potencialmente perigosas para indivíduos, organizações e até mesmo estados, e isso é difícil de prever com suficiente antecipação. A falta de transparência acerca da forma com que dados são agregados e analisados, combinada com a dificuldade em se prever quais informações podem vir a se tornar perigosas, leva a situações em que indivíduos (e mesmo organizações) tenham pouca percepção acerca dos efeitos potencialmente deletérios do avanço do uso da CSS.

A aplicação de CSS pode ser voltada a coisas aparentemente inofensivas, como propaganda de produtos de consumo, mas, quando aplicada às áreas de antropologia social e ciência política, pode ser usada para atentar contra a democracia. Combinando essas aplicações, pode-se chegar a cenários em que CSS pode ser utilizada para dirigir propaganda política (não apenas eleitoral), selecionar quais informações podem chegar a determinados grupos, quais não podem etc. Isso torna-se particularmente grave

quando está ficando claro que as informações geradas estarão acessíveis aos governos, àqueles capazes de pagar por elas ou às empresas que conseguem reunir grandes volumes de dados, cujos exemplos clássicos são Facebook e Google [Oboler *et al*, 2012].

Conforme os atuais Termos de Serviço do Google, implementados em 2012 e aos quais seus usuários não tem a opção de se furtarem [Google, 2012], a empresa pode avaliar seus usuários, combinando e analisando dados coletados em todos os seus serviços, como por exemplo, histórico de pesquisa, utilização do Google+, conexões a redes sociais, uso do Gmail, compras *online* pagas com Google Wallet, arquivos de fotos etc. – as práticas do Google acerca de privacidade são frequentemente questionadas [Estado, 2013].

Com base nessa avaliação, os usuários poderiam ser direcionados para vídeos do You Tube e notícias do Google News (também vídeos e notícias poderiam ser “ocultados” do usuário) de forma a mostrar que um determinado partido político concorda com as opiniões desse usuário (ou que outro não concorda), influenciando sua maneira de pensar, por exemplo.

Oboler (2012), diz que tais direcionamentos poderiam ser feitos de maneira sutil, pois a CSS permite prever a eficácia de mensagens diferentes para pessoas diferentes – assim mensagens inócuas poderiam ser encaminhadas em meio a outras mais “agressivas”, de forma a não caracterizar uma atuação parcial. Esses serviços poderiam ser usados não só por uma empresa como o Google, mas também vendidos a terceiros, influenciando resultados de eleições, o que é antidemocrático. Eleições envolvem frequentemente dezenas ou mesmo centenas de milhões de pessoas, não sendo, por essa razão, surpresa o fato de que elas estão entre os mais estudados fenômenos sociais e consequentemente um campo naturalmente candidato à aplicação de CSS [Fortunato e Castellano, 2012].

Jones *et al* [2013] concluíram ser possível estabelecer a força da ligação entre pessoas simplesmente analisando suas interações via Facebook, sem considerar os atributos dessas pessoas. Identificando ligações fortes, é possível também influenciar comportamentos, desde os relativamente inócuos como recomendação de produtos como àqueles ligados à política.

A aplicação de CSS, para o bem ou para o mal, é limitada pela disponibilidade de dados. Temas ligados à captura de dados a serem utilizados por aplicações ligadas à CSS e sobre o acesso às informações por elas geradas devem passar a ser consideradas questões chave em termos de políticas públicas.

Ao limitar a aquisição, compartilhamento e uso de dados, e pela sensibilização da sociedade para as implicações de sua disponibilidade, especialmente em termos éticos, é possível limitar os problemas aqui relatados, hoje ainda relativamente raros, mas que tendem a aumentar exponencialmente se nada for feito pela sociedade. O uso da CSS pode ser um grande benefício da busca por conhecimento, mas como acontece em relação a todos os avanços científicos, a sociedade precisa estar consciente de seus riscos.

6. Considerações finais

Considerando as questões aqui apresentadas, observa-se que o crescimento deste campo de conhecimento é evidente, bem como, os benefícios envolvidos. Contudo, assim como em outras ciências, faz-se necessária a discussão mais ampla acerca das questões éticas e os riscos inerentes a este contexto.

Na ótica da tecnologia, o fenômeno Big Data está sendo muito positivo, pois motivou avanços na área de persistência de dados, tanto no que diz respeito a *hardware* como *software*. Assim como acontece no campo da moda, as empresas de tecnologia estão vivendo, de certa forma, uma volta ao passado, como acontecia outrora com os *mainframes*: os principais *players* estão comercializando *hardware* para BI/BA com *software* embarcado, na perspectiva de alcançar melhor *throughput* nas operações de recuperação de informação.

De modo complementar, os novos paradigmas de persistência, da família NoSQL, estão contrapondo a teoria de que um sistema gerenciador de banco de dados único é quase sempre suficiente para atender as necessidades de armazenamento e recuperação de dados de uma organização; soluções híbridas parecem melhor atender demandas em tempo de Big Data, que envolvem questões de escalabilidade em ambientes distribuídos e heterogêneos.

Assim como as questões tecnológicas evoluem, é importante evoluir na mesma cadência a discussão sobre os aspectos éticos e os riscos envolvidos.

O assunto é complexo e globalizado, na medida que a tecnologia está derrubando fronteiras geográficas. Empresas geram armazéns de dados globalizados. Mesmo que um país determine leis que regulamentem o uso de dados para CSS, tal legislação está limitada às fronteiras geográficas daquele país. Não são casuais os conflitos que a Google tem em países como China e França.

Governos a parte, a construção de perfis individuais com base em conteúdos digitais, bem como o seu uso nas diversas formas de aplicação, compõem um tema que carece de discussão mais aprofundada na sociedade.

Referências Bibliográficas

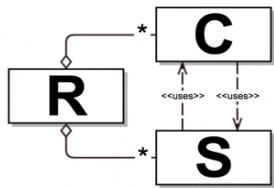
- Agarwal, R., Gupta, A. K. e Kraut, R. (2008). Overview - the interplay between digital and social networks. In *Information Systems Research*, vol. 19, nº. 3.
- Atzori, L., Iera, A. e Morabito, G. (2010). The Internet of Things: A survey. In *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 54, ed. 15.
- Battibugli, A. O. (2013). Big Data antecipa a morte do currículo. In *EXAME*, edição de 26.05.2013.
- Cioffi-Revilla, C. Computational Social Science. (2010). In *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, nº 3.
- Chui, M., Löffler, M. e Roberts, R. (2010). The internet of things. In *McKinsey Quarterly*, v. 2.

- Clifford, S. (2012) Retail frenzy: prices on the Web change hourly. In *The New York Times*, edição de 30.11.2012.
- Economist. (2010). The data deluge. In *The Economist*, edição de 27.02. 2010.
- Estado. (2013). Google Play tem privacidade questionada. In *O Estado de S. Paulo*, edição de 16.02.2013.
- Fortunato, S. e Castellano, C. (2012). Physics peeks into the ballot box. In *Physics Today*, vol. 65, nº 10, 2012.
- Global Pulse. (2012). Big Data for development: challenges & opportunities. Nova Iorque: Global Pulse.
- Gnatovich, R. (2006). Business Intelligence versus Business Analytics - What's the difference?, disponível em http://www.cio.com/article/18095/Business_Intelligence_Versus_Business_Analytics_What_s_the_Difference, acessado em 03.07.2013.
- Google. (2012). Termos de serviço do Google, disponível em <http://www.google.com/intl/pt-BR/policies/terms/>, acessado em 14.02.2013.
- Jones, J. J., Settle, J. E., Bond, R. M., Fariss, C. J., Marlow, C. e Fowler, J. H. (2013). Inferring tie strength from online directed behavior, disponível em <http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0052168>, acessado em 14.02.2013.
- King, G. (2013). Restructuring the Social Sciences: reflections from Harvard's Institute for Quantitative Social Science, disponível em <http://gking.harvard.edu/files/gking/files/iqss.pdf>, acessado em 13.01.2013.
- Lohr, S. (2012). “The Age of Big Data” http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&scp=1&sq=Big%20Data&st=cse, acessado em 02.01.2013.
- Mcafee, A. e Brynjolfsson, E. (2012). Big Data: The Management Revolution. In *Harvard Business Review*, edição de outubro de 2012.
- Moraes, M. (2012). Big Brother Obama. In *InfoExame*, edição de dezembro de 2012.
- NoSQL. (2013). Your Ultimate Guide to the Non - Relational Universe, disponível em <http://nosql-database.org>, acessado em 05.07.2013.
- Oboler, A., Welsh, K. e Cruz, L. (2012). The danger of Big Data: social media as computational social science. In *First Monday*, vol 17, nº 7.
- Ortega Y Gasset, J. (2004) Meditaciones del Quijote - in: Obras Completas, vol. I. Madrid: Taurus.
- Rossouw, L. (2012). Big Data – Grandes Oportunidades. In *Gen Re – Risk Insights*, vol. 16, nº 2.
- Selltiz, C., Wrightsman, L. S. e Cook, S. W. (2001). Métodos de pesquisa nas relações sociais. 2. ed. São Paulo: EPU.
- Taube, B. (2012). Leveraging Big Data and real-time analytics to achieve situational awareness for smart grids (white paper). Redwood City: Versant Corporation U.S. Headquarters.

Taurion, C. (2011). Big Data: nova fronteira em gerenciamento de dados, disponível em http://www.ibm.com/developerworks/mydeveloperworks/blogs/ctaurion/entry/big_data_nova_fronteira_em_gerenciamento_de_dados?lang=en, acessado em 17.01.2013.

Tene, O. e Polenetsky, J. (2012). Privacy in the age of Big Data - a time for big decisions, disponível em <http://www.stanfordlawreview.org/online/privacy-paradox/big-data>, acessado em 14.01.2013.

Zikopoulos, P., De Roos, D., Parasuraman, K., Deutsch, T., Giles, J. e Corrigan, D. (2012). Harness the power of Big Data - The IBM Big Data Platform. Emeryville: McGraw-Hill Osborne Media.



Fortalecimento Do Protocolo De Criptografia Quântica BB84

Nathália Costa e Silva, Rafael Hissato Minomiya, Luciano Silva

Faculdade de Computação e Informática, Universidade Mackenzie, São Paulo

nat.thalia.cs@gmail.com, minomiyarafael@gmail.com

luciano.silva@mackenzie.br

Abstract. An alternative to classical cryptography methods is the quantum cryptography, whose security is assured by quantum physics laws, and it can be simulated in optical fiber. The BB84 protocol is a quantum distribution key protocol which uses two bases for polarization of photons, providing half of the information for an eavesdropper on each measure. In order to reduce the information intercepted by the eavesdropper, it was proposed a strengthening for this protocol, and, to achieve the proposed objectives on this project, there were added two new bases for polarization in order to complicate the eavesdropper's measurements, reducing the information acquired by him. To avoid damaging the protocol, it was necessary to introduce a different method to do the measurements and polarizations of the photons using a cyclic key, composed by pairs of the bases. The results were satisfactory, since the goal of strengthening the security of BB84 protocol was achieved by decreasing the amount of information that an eavesdropper is able to get without being detected, and it wasn't necessary neither to increase the quantity of information which goes by the quantum channel, nor to decrease the information the receiver acquires on his measurements.

Resumo. Uma alternativa aos métodos de criptografia clássica é a criptografia quântica, cuja segurança é garantida pelas leis da física quântica, e pode ser simulada em fibra ótica. O protocolo BB84 é um protocolo de distribuição de chaves quântica que utiliza duas bases para polarização dos fôtons, fornecendo, assim, metade da informação para um intruso a cada medida. Com a finalidade diminuir a informação interceptada por um intruso, foi proposto um fortalecimento deste protocolo, e, para alcançar os objetivos propostos neste trabalho, foram adicionadas duas novas bases para polarização, para dificultar as medições de um intruso, diminuindo, assim, a informação adquirida por ele. Para não prejudicar o protocolo, foi necessário introduzir um método diferente para realizar as polarizações e as medições dos fôtons, utilizando uma chave cíclica, formada por pares de bases. Os resultados foram satisfatórios, uma vez que o objetivo de reforçar a segurança do protocolo BB84 foi alcançado, diminuindo a quantidade de informação que um intruso pode adquirir sem ser detectado, sem a necessidade de aumentar a quantidade de informação que tráfega no canal quântico, nem diminuir a informação que o receptor adquire com suas medições.

1 Introdução

A Criptografia é a ciência cujo objetivo é proteger informações privadas e assegurar a integridade dos dados e a autenticidade das partes envolvidas. A segurança dos métodos clássicos de criptografia é garantida pela dificuldade de problemas matemáticos, como a fatoração de números inteiros, utilizada pelo RSA, e o problema do logaritmo discreto, usado em curvas elípticas. Com o surgimento da computação quântica e dos algoritmos quânticos de Shor para fatoração de números inteiros e cálculo de logaritmos discretos, a criptografia clássica ficou, pelo menos em teoria, vulnerável. Ainda que não exista um computador quântico para quebrar os métodos de criptografia clássica, alternativas já são estudadas (BRUSS *et al.*, 2007).

Uma alternativa é a criptografia quântica, ou distribuição de chaves quântica. Segundo Marquezino (2003), é provavelmente segura a distribuição de chaves quânticas utilizando estados não-ortogonais, com um protocolo como o BB84, e se houver espionagem, o canal será perturbado, causando um aumento detectável na taxa de erro. Além disso, na mecânica quântica, não é possível clonar um *qubit*, portanto a segurança da criptografia quântica é garantida pelas leis da física quântica (BRUSS *et al.*, 2007).

O protocolo BB84 é um protocolo no qual Alice utiliza um canal quântico para enviar *bits* codificados utilizando fôtons polarizados na base retilínea (0° ou 90°) ou diagonal (45° ou 135°), aleatoriamente, para Bob, que faz medições nos *qubits* em alguma das duas bases, também aleatoriamente. O protocolo consiste em garantir que Alice e Bob obtenham uma chave única e que um intruso seja detectado (MARQUEZINO, 2003).

O objetivo deste trabalho é propor uma forma de fortalecer o protocolo de distribuição de chaves quântica BB84 acrescentando duas bases para polarização além das bases retilínea e diagonal, sem diminuir a quantidade de informação obtida por Bob, porém diminuindo a informação que um possível intruso pode conseguir.

O artigo está dividido em computação quântica, informação quântica, protocolo BB84, fortalecimento do protocolo BB84, conclusões e trabalhos futuros. Nos dois primeiros tópicos foram definidos conceitos relevantes sobre computação quântica e informação quântica para, em seguida, explicar o funcionamento do protocolo BB84, no terceiro tópico. A seção do fortalecimento do protocolo BB84 esclarece e justifica a proposta do trabalho e as decisões tomadas em relação a ela. Por fim, o tópico conclusões e trabalhos futuros mostra se o objetivo do trabalho foi alcançado e sugere pesquisas posteriores possíveis sobre o fortalecimento.

2 Computação Quântica

A computação quântica refere-se ao processamento de computadores quânticos, os quais utilizam a álgebra quântica, baseada na teoria da mecânica quântica. Uma das diferenças entre a computação clássica e a computação quântica é a unidade de informação utilizada: na clássica, utiliza-se o *bit* (*binary digit*), representado numericamente por “0” ou “1”, que podem ser interpretados respectivamente como tensão baixa ou alta, desligado ou ligado, etc.; já na computação quântica, é utilizado o *qubit* (*quantum bit*), que, diferente do *bit*, pode ser interpretado como $|0\rangle$ ou $|1\rangle$, análogos aos estados clássicos 0 e 1, ou uma superposição dos dois estados (MELO; CHRISTOFOLETTI, 2003). A notação padrão para estados

quânticos, representada por “| >”, é chamada notação de Dirac (NIELSEN; CHUANG, 2010).

O *qubit*, que, como visto anteriormente, é usado na computação quântica como unidade de informação, é um objeto quântico e segue as leis que regem o mundo micro, da mecânica quântica. O *bit* clássico pode ser representado fisicamente pela tensão elétrica, já os *qubits* são representados por objetos quânticos com estados bem distintos, como a polarização do fóton, *spins* quânticos, átomos de dois níveis como mostrado na Figura 1, dentre outros (NIELSEN; CHUANG, 2010).

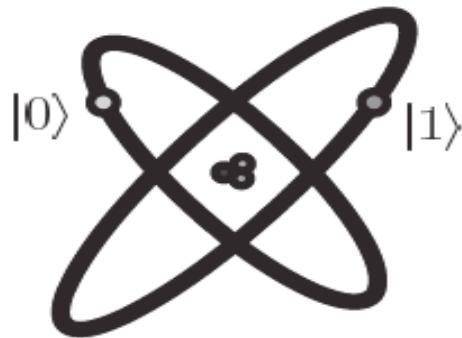


Figura 1: *Qubit* representado por dois níveis eletrônicos em um átomo.

Visto que os *qubits* são superposições de dois estados, dois *qubits* podem ser uma combinação de todos os números de dois *bits* ao mesmo tempo, três *qubits* podem ser uma combinação de todos os números de três *bits* ao mesmo tempo, e assim por diante. Com isso, têm-se o chamado paralelismo quântico (FERNANDES et al, 2007).

Formalmente, o *qubit* é um vetor em um espaço de Hilbert (GRIFFITHS, 2005) de duas dimensões, os estados $|0\rangle$ e $|1\rangle$ são denominados estados da base computacional e formam uma base ortonormal nesse espaço vetorial. O *qubit* $|\Psi\rangle$ é representado da seguinte forma:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle ,$$

sendo que $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$, ou seja, o estado quântico $|\Psi\rangle$ pode colapsar para o estado $|0\rangle$ com probabilidade $|\alpha|^2$ e para o estado $|1\rangle$ com probabilidade $|\beta|^2$. Em um *qubit*, os valores “0” e “1” podem ser armazenados ao mesmo tempo com a sobreposição. O estado de um *qubit*, expresso geometricamente, é a rotação de um vetor na esfera de Bloch (NIELSEN; CHUANG, 2010), como mostra a Figura 2, próxima página, e pode ser representado da seguinte maneira:

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle .$$

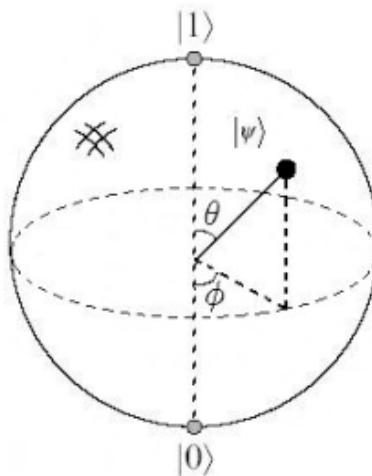


Figura 2: Representação de um *qubit* na esfera de Bloch.

Um sistema físico muda com o tempo, o mesmo acontece com um *qubit* $|\Psi\rangle$. A evolução de um sistema quântico é descrita por um operador unitário, ou seja, sendo o estado inicial do sistema $|\Psi_1\rangle$ e o estado final $|\Psi_2\rangle$, existe um operador unitário U que satisfaça $|\Psi_2\rangle = U|\Psi_1\rangle$. Um operador em um espaço de Hilbert de duas dimensões para um único *qubit* pode ser representado por uma matriz de dimensão 2x2 (KAYE et al, 2007).

Visto que os *qubits* são representados por vetores no espaço de Hilbert, as portas lógicas, que na computação clássica são circuitos, na computação quântica são operadores, isto é, matrizes, os quais são aplicados a esses vetores (FERNANDES et al, 2007).

Por outro lado, durante uma medição, o processo não é unitário. Suponha um sistema com N estados, $|0\rangle, |1\rangle, \dots, |N-1\rangle$, e um aparato que seja capaz de distingui-los. A medição é o processo pelo qual se obtém como resultado uma descrição clássica de um estado quântico, ou seja, o aparato terá como resposta i , com probabilidade $|\alpha_i|^2$ e o estado do sistema convergirá para $|i\rangle$ (KAYE et al, 2007). Em outras palavras, o simples fato de medir o estado de um *qubit* $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ destrói o estado quântico, retornando sempre $|0\rangle$ ou $|1\rangle$ nas medições, com as respectivas probabilidades $|\alpha|^2$ ou $|\beta|^2$, e nunca uma sobreposição dos dois estados (NIELSEN; CHUANG, 2010).

Concluindo, os três axiomas da mecânica quântica são a superposição, a qual diz que o estado quântico de um sistema é um vetor unitário em um espaço de Hilbert, a medição, a qual declara que, ao fazer uma medida, o estado colapsa para uma das bases com certa probabilidade, e a evolução unitária, a qual exprime que a evolução de um estado quântico no tempo corresponde a uma rotação no espaço de Hilbert.

Para entender a computação quântica, é preciso entender como a mecânica quântica funciona quando há um sistema em que haja interação entre dois ou mais *qubits*, isso será melhor explicado ao longo do texto. Quando dois *qubits* são tratados como um único sistema, diz-se que o espaço do sistema combinado é o produto tensorial dos dois espaços, isto é, esteja o primeiro *qubit* no estado $|\Psi_1\rangle$ e o segundo no estado $|\Psi_2\rangle$, o estado combinado é $|\Psi_1\rangle \otimes |\Psi_2\rangle$, que pode ser escrito $|\Psi_1\rangle |\Psi_2\rangle$ ou $|\Psi_1\Psi_2\rangle$ (KAYE et al, 2007).

3 Informação Quântica

A informação é uma quantidade abstrata e, para processar, armazenar ou transmitir uma informação é necessário codificar o conteúdo para um sistema físico e aplicar as leis da física para processar a informação. A informação na computação clássica é codificada em *bits*, que são representadas, por exemplo, por tensão alta ou tensão baixa, e que, portanto, obedecem as leis da mecânica clássica. Para processar uma informação quântica, é necessário um objeto quântico, por exemplo os átomos, elétrons, fôtons, ou qualquer outra partícula a nível atômico. Na computação quântica a informação é representada por *qubits*, apresentado no tópico anterior, que são regidos pelas propriedades da mecânica quântica.

A física clássica não é capaz de explicar a mecânica do mundo subatômico, o que torna os *qubits* diferentes dos *bits*. Por exemplo, na teoria da informação quântica, não é possível copiar o estado quântico $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ de um *qubit* e produzir duas cópias $|\Psi\rangle |\Psi\rangle$ sem ter conhecimento dos valores de α e β , devido a linearidade da mecânica quântica, como será observado a seguir.

Suponha U como uma operação unitária que pode clonar um *qubit*. Então U pode clonar os estados $|0\rangle$ e $|1\rangle$:

$$U|0\rangle = |00\rangle \quad (1)$$

$$U|1\rangle = |11\rangle \quad (2).$$

Como uma operação unitária pode ser representada por uma matriz, podemos aplicar U em um *qubit* genérico $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ e resultará em $U|\Psi\rangle = \alpha U|0\rangle + \beta U|1\rangle$. Substituindo as expressões 1 e 2, como segue:

$$U(|\Psi\rangle) = \alpha|00\rangle + \beta|11\rangle \quad (4).$$

Se a operação U clonar um *qubit* deverá apresentar o seguinte resultado:

$$U(|\Psi\rangle) = |\Psi\rangle |\Psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \quad (5).$$

O resultado da expressão 4 é diferente da expressão 5, concluindo a propriedade quântica da impossibilidade de se clonar um *qubit*. Esta propriedade, chamada de teorema da não-clonagem, tem vantagens e desvantagens no processamento da informação quântica. Por não ser possível clonar um *qubit*, a transmissão de informação ganha um reforço em segurança, por outro lado, não é possível efetuar uma correção de erro em um *qubit* como nos *bits* clássicos, armazenando uma cópia de segurança, por exemplo (VENDRAL, 2006).

Outra propriedade da mecânica quântica que a mecânica clássica não está apta para responder é o fato de que as partículas ou sistemas subatômicos são capazes de se emaranhar, o que significa que se dois sistemas estiverem emaranhados, os valores de certas propriedades de um sistema estarão correlacionados com os valores que as propriedades assumirão do outro sistema, um interferindo diretamente no resultado do outro, mesmo que separados espacialmente (MCMAHON, 2008). Em outras palavras, diz-se que dois *qubits* estão emaranhados se não for possível escrevê-los como um produto tensorial de outros estados (PAPADAKOS, 2001).

O emaranhamento, por outro lado, pode ser uma alternativa para fazer uma medição em um *qubit* sem destruir seu estado quântico, pois, ao medir o primeiro *qubit*, ele converge para

um valor, e, simultaneamente, o segundo *qubit* também converge, com isso pode-se determinar seu valor sem observá-lo (FERNANDES et al, 2007).

Um exemplo de emaranhamento bastante utilizado é o estado de Bell, ou par de Bell, que possui quatro configurações diferentes, porém com as mesmas propriedades:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle,$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle,$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle.$$

O estado de Bell é uma superposição com mesma amplitude para os estados $|00\rangle$ e $|11\rangle$ e tem como propriedade os resultados correlacionados, isto é, ao medir o primeiro *qubit*, sabe-se o valor do segundo *qubit* sem realizar uma medição. Em outras palavras, a probabilidade de se obter 0 é $\frac{1}{2}$ e a probabilidade de se obter 1 é $\frac{1}{2}$, porém, ao fazer a medição no primeiro *qubit*, se for encontrado 0, sabe-se que o segundo *qubit* será 0 com probabilidade 1 e seu estado será $|00\rangle$, ou, se o resultado do primeiro *qubit* for 1, o segundo *qubit* também será 1 e seu estado será $|11\rangle$. Os resultados são coordenados, independentemente da distância a que são separados os dois *qubits*. Uma das utilidades do par de Bell é o teletransporte quântico (NIELSEN; CHUANG, 2010), explicado a seguir.

Como foi demonstrado, é impossível copiar um *qubit* desconhecido segundo o teorema de não-clonagem, porém é possível transmitir um estado quântico de um lugar para outro através do teletransporte quântico.

O teletransporte quântico é um protocolo que utiliza a propriedade do emaranhamento quântico para teletransportar um *qubit* de Alice para Bob (KAYE et al, 2007), como detalhado a seguir e ilustrado na Figura 3.

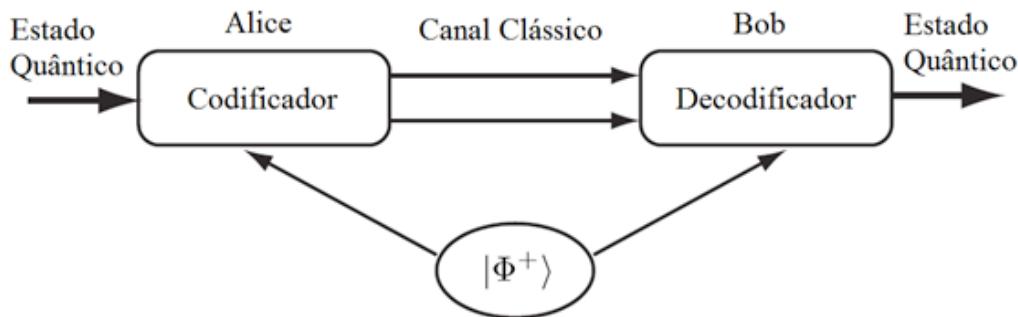


Figura 3: Teletransporte quântico.

Alice e Bob, em algum momento no passado, compartilharam um par de Bell no estado $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice, então, quer enviar um *qubit* $|\psi\rangle$ em um estado desconhecido a Bob, ou seja, um *qubit* $|\psi\rangle = a|0\rangle + b|1\rangle$, entretanto ela não pode fazer uma cópia deste estado, tampouco pode medi-lo para obter os valores de a e b visto que, ao fazer a medição, obtém-se 0 com a probabilidade $|a|^2$ ou 1 com a probabilidade $|b|^2$, e não os valores desejados. Além disso, realizando a medição, o estado do *qubit* torna-se o estado para o qual ele convergiu, não sendo possível repetir o experimento.

O estado inicial dos três *qubits* obtidos por Alice e Bob é:

$$|\Psi\rangle = |\Phi^+\rangle = a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle.$$

Alice mede seus dois *qubits*, o *qubit* que deseja mandar e o seu *qubit* do par de Bell, seu estado após a medição é um entre os estados a seguir:

$$\begin{aligned} &|00\rangle (a|0\rangle + b|1\rangle), \\ &|01\rangle (a|1\rangle + b|0\rangle), \\ &|10\rangle (a|0\rangle - b|1\rangle), \\ &|11\rangle (a|1\rangle - b|0\rangle), \end{aligned}$$

cada um com probabilidade $\frac{1}{4}$.

O fato de Alice ter feito a medida faz com que o estado colapse para uma das quatro possibilidades e produza dois *bits* clássicos, que são enviados a Bob. Se necessário, Bob aplica operações em seu *qubit* utilizando portas quânticas, e obtém como resultado o estado $|\Psi\rangle = a|0\rangle + b|1\rangle$, estado que Alice queria enviar a princípio (STEANE, 1997).

O teletransporte quântico não contradiz o teorema de não-clonagem, pois a informação original, do lado de Alice, é destruída para ser transmitida e recebida do lado de Bob (NAKAHARA; OHMI, 2008).

Concluindo, o teletransporte quântico permite que Alice envie a Bob um estado quântico apenas utilizando *qubits* emaranhados - o par de Bell -, enviando dois *bits* clássicos e fazendo medições locais, o que não exige um canal quântico de comunicação e pode ser realizado a longas distâncias. Pode-se dizer, portanto, que Alice envia para Bob um estado quântico sem enviar nenhuma informação quântica (KAYE et al, 2007).

Uma das aplicações da teoria da informação quântica é a criptografia quântica. A criptografia tem como principal função estabelecer uma comunicação segura entre duas partes, Alice e Bob, e evitar que um provável intruso, Eve, consiga obter informações dessa comunicação. A criptografia quântica utiliza a mecânica quântica para garantir uma distribuição de chaves segura em um canal público, as quais serão usadas posteriormente em métodos de criptografia de chave privada. Por isso, a criptografia quântica também é chamada de distribuição de chave quântica (FERNANDES et al, 2007).

A mecânica quântica pode ser utilizada para garantir a segurança da criptografia quântica, pois, como foi definido anteriormente, as informações não podem ser copiadas, segundo o teorema de não-clonagem, e qualquer ganho de informação de Eve pode perturbar o sistema. O primeiro protocolo de distribuição de chave quântica foi o Protocolo BB84, apresentado a seguir (PAPADAKOS, 2001).

4 Protocolo Bb84

Em 1984, foi publicado o primeiro método de criptografia quântica, ou seja, o primeiro protocolo de distribuição de chaves quântica, desenvolvido por Charles Henry Bennet e Gilles Brassard, o que originou a sigla BB84 (MARQUEZINO, 2003). Um protocolo de distribuição de chaves quântica, ou DCQ (do inglês, *quantum key distribution* ou QKD), tem a função de estabelecer uma conexão segura na qual Alice usa um canal quântico para

enviar *qubits* para Bob, os quais serão utilizados para formar chaves secretas, que serão usadas em outros métodos de criptografia, usados para o envio de mensagens (BRUSS et al, 2007).

Os protocolos de distribuição de chaves quântica, assim como o BB84, utilizam dois canais de comunicação, um canal clássico e um canal quântico, que estão ilustrados na figura 4 (NAKAHARA; OHMI, 2008).

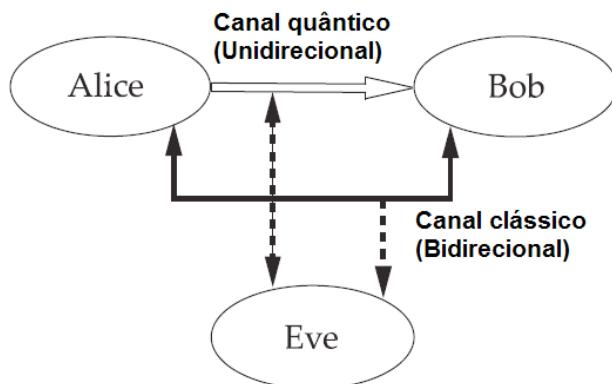


Figura 4: Canais utilizados no protocolo BB84.

O canal clássico é utilizado para transportar a mensagem criptografada, utilizando a chave estabelecida pelo protocolo BB84, por uma rede clássica como, por exemplo, a internet. Já o canal quântico se diferencia por transmitir apenas estados quânticos, como fôtons polarizados, isto é, no caso de um protocolo DCQ, é utilizado para estabelecer um canal seguro para troca de chaves secretas, com a capacidade de detectar um intruso no meio da comunicação. O canal quântico não é utilizado para troca de mensagens por não ser tão eficaz em relação ao tempo e custo.

A seguir será descrito com mais detalhes o funcionamento do protocolo BB84 utilizando canais de comunicação ideais, sem ruído.

Suponha que um transmissor, Alice, queira transmitir uma mensagem secreta para um receptor, Bob, e precisa evitar que um intruso, Eve, intercepte a mensagem. Antes de iniciar o protocolo, Alice e Bob precisam ter conhecimento de uma pequena chave secreta para autenticação, para evitar que Eve tente se passar por um dos dois ao iniciar o protocolo, esta chave será usada apenas no início do protocolo e depois será descartada, o próprio protocolo ficará encarregado de gerar novas chaves de autenticação.

Após a verificação de autenticidade de Alice e Bob, usando a chave secreta para o início do protocolo, Alice irá escolher aleatoriamente uma sequência de *bits* e uma sequência de bases para polarização dos fôtons, que podem ser diagonal (x) ou retilínea (+), sendo uma base para cada *bit*. Na base retilínea, os fôtons são polarizados em 0 ou 90 graus e, na base diagonal, são polarizados em 45 ou 135 graus. Em seguida, Alice envia os *qubits* para Bob na forma de fôtons polarizados de acordo com o valor de cada *bit* e sua respectiva base, seguindo o padrão:

- para enviar o *bit* 0, o fôton deverá ser polarizado em 0° na base retilínea ou 45° na base diagonal;
- para enviar o *bit* 1, o fôton deverá ser polarizado em 90° na base retilínea ou 135° na base diagonal.

Para efetuar a leitura de cada *qubit*, Bob deverá escolher aleatoriamente uma das bases, diagonal (x) ou retilínea (+), e guardar as informações sobre qual base foi usada e qual o resultado de cada *qubit* medido, sendo que as informações obtidas só estarão corretas quando Bob fizer a medição do *qubit* na mesma base que Alice usou para codificá-lo, caso contrário, o resultado será aleatório.

Após a medição de todos os *qubits*, Bob terá uma sequência de *bits*, chamada de “chave bruta” (*raw key*). Os *bits* enviados por Alice compõem sua chave bruta, que é diferente em 25% da chave bruta de Bob, devido aos erros das medições incorretas.

A criação da chave bruta é conhecida como o primeiro passo do Algoritmo BB84. Neste passo, verifica-se que as chaves brutas combinam em 75% dos *bits*, porém $\frac{1}{3}$ dos *bits* corretos foram obtidos aleatoriamente, devido às medições que foram realizadas utilizando bases erradas e geraram resultados aleatórios. Como Alice enviou para Bob apenas as bases corretas na medição, não é possível para Bob identificar os *bits* que foram obtidos corretamente por meio de bases erradas, por isso são descartados, restando 50% da chave bruta.

Em seguida, é executado o segundo passo do protocolo, a reconciliação de bases. Nesta etapa, Alice envia para Bob, utilizando o canal clássico, as bases que ela utilizou para a geração de sua chave bruta e Bob envia para Alice a sequência de polarizadores que ele utilizou nas medições dos fótons, mas sem revelar o resultado das medições. Ambos comparam as duas bases, as que Alice utilizou para polarizar os fótons e as que Bob usou para medi-los, e descartam as bases divergentes. Com isso, 50% da chave é descartada, restando apenas os valores que Bob mediou utilizando as mesmas bases de Alice. Os *bits* restantes formam a chamada “chave filtrada” (*sifted key*).

No terceiro passo do protocolo é feita a verificação de intrusos. Utilizando a chave filtrada, é possível detectar se algum intruso interceptou a comunicação verificando a taxa de erro. A taxa de erro dos *bits* quânticos (do inglês *quantum bit error rate*, ou QBER) é utilizada para verificar a porcentagem de erro entre as chaves filtradas. Alice e Bob divulgam um subconjunto aleatório da chave filtrada e calculam o QBER que, teoricamente, deveria ser zero, supondo uma comunicação ideal, sem ruído. Se Eve fizer a medição de algum *qubit* antes de Bob, Eve interferirá no sistema e introduzirá ruído nas medições de Bob, podendo, assim, ser detectado antes que Alice e Bob transmitam qualquer informação sigilosa. Se for detectado algum intruso na comunicação, Alice e Bob voltam ao início do protocolo e começam novamente. Caso contrário, os *bits* usados para verificação são descartados e o protocolo segue para o próximo passo.

No quarto passo do protocolo, é utilizada quando não há um canal de comunicação ideal, ou seja, o protocolo é realizado em um canal com ruído. Esta etapa corrige os erros encontrados na terceira etapa, aplicando algoritmos de correção de erros, com a finalidade de corrigir os ruídos introduzidos pelo canal de comunicação ou pelos equipamentos utilizados na criptografia quântica. Esses ruídos são comuns na prática, não há como garantir 100% que uma comunicação à distância não tenha ruídos. É importante salientar que, na prática, se Eve fizer medições em parte da comunicação entre Alice e Bob, a terceira etapa do protocolo pode confundir a interferência de Eve com um ruído de canal ou do sistema e, chegando na quarta etapa, esses ruídos serão corrigidos, assim Eve não será detectada.

Para garantir que Eve não consiga informação suficiente para colocar em risco a comunicação, é aplicada a quinta etapa do protocolo, denominada ampliação de privacidade. Nesta etapa, a chave é reduzida para minimizar a informação obtida por Eve (MARQUEZINO, 2003).

A segurança do protocolo BB84 é garantida pelas propriedades da mecânica quântica como o teorema da não clonagem, o que impossibilita que Eve consiga fazer uma cópia do *qubit*, além disso, se Eve fizer uma medição, ele perturbará o sistema. Outro fato que garante a segurança do protocolo é o terceiro passo, que detecta a presença de ruídos no canal quântico, acusando a intrusão de Eve e, caso não seja detectada por interceptar apenas parte da informação, o quinto passo, o qual amplifica a privacidade da chave, reduzindo a informação de Eve para valores aceitáveis (MARQUEZINO, 2003).

A Tabela 1 exemplifica o uso do protocolo BB84:

Tabela 1: Tabela para exemplificar o funcionamento do protocolo BB84.

Bits enviados	1	0	0	1	0	1	1	1	0	0	1	0	1	0	1
Base Alice	+	+	x	x	+	x	+	x	x	x	+	+	+	x	+
Base Bob	x	+	x	x	x	+	+	x	+	x	+	x	x	+	+
Chave		0	0	1			1	1		0	1				1

A Tabela 1 ilustra um exemplo simplificado do funcionamento do protocolo BB84. A primeira linha da tabela mostra a chave bruta de Alice, ou seja, a sequência de *bits* aleatórios que Alice escolheu para enviar a Bob, e a segunda linha mostra as polarizações que ela usou para codificar cada *bit*, a polarização retilínea está representada pelo símbolo + e a polarização diagonal pelo símbolo x. A terceira linha apresenta as polarizações usadas por Bob para medir cada fóton recebido. As três primeiras linhas referem-se ao primeiro passo do protocolo.

A quarta linha da tabela é correspondente ao segundo passo do protocolo, no qual Alice envia a Bob quais polarizações foram utilizadas para codificar os *bits* e Bob envia à Alice as polarizações usadas para medi-los. Com essas informações, Alice e Bob descartam os *bits* que não foram medidos na mesma base em que foram codificados, formando, assim, a chave filtrada. Neste exemplo, o primeiro, o quinto, o sexto, o nono, o décimo segundo, o décimo terceiro e o décimo quarto *bits* foram descartados por serem resultados aleatórios, resultando na chave filtrada 00111011.

Este exemplo é apenas uma ilustração simplificada. No protocolo completo, Alice e Bob ainda fariam as outras etapas, comparando parte das chaves filtradas obtidas para verificação de intrusos, correção de erros e amplificação da privacidade. Além disso, na prática o número de *bits* usados seria maior.

Pode-se observar que, sem a interferência de um intruso, Bob só obtém a informação correta nos *qubits* que forem medidos na mesma base que Alice os codificou. Caso contrário, as informações obtidas por Bob são aleatórias e, portanto, descartadas. A Figura 5, próxima página, ilustra os possíveis casos de medições realizadas.



Figura 5: Casos possíveis sem interferências de um intruso.

É possível observar que metade da informação é descartada por não ter sido medida na base correta. Portanto, Alice e Bob aproveitam apenas 50% dos *bits* enviados, isto é, a chave filtrada tem metade do tamanho da chave bruta.

Supondo que não haja ruído no canal, mas que um intruso esteja fazendo uma espionagem e reenviando os *qubits* para Bob, as possibilidades de medidas são mostradas na figura 6.

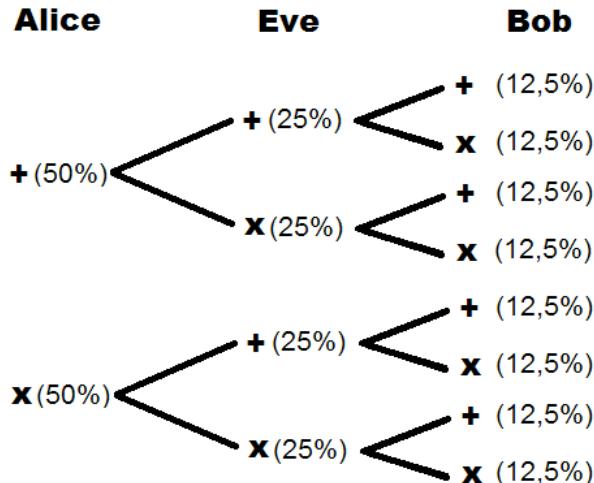


Figura 6: Casos possíveis com a interferência de um intruso.

Neste caso, Eve possui informações corretas quando suas medições forem feitas na mesma base que Alice fez as polarizações, portanto Eve consegue metade da informação. Por outro lado, quando Eve medir na base errada mas Bob fizer a medição na base correta, Bob, na verdade, estará recebendo informações aleatórias, portanto Eve acrescenta uma taxa de erro.

A chave filtrada, como dito anteriormente, é composta pelos *bits* que forem codificados por Alice e medidos por Bob nas mesmas bases, então, mesmo que Eve faça a medição em uma base diferente, esses *bits* farão parte da chave filtrada, como mostra a Tabela 2, próxima página, porém os valores serão aleatórios.

Tabela 2: Chave filtrada em caso de espionagem.

Base utilizada por Alice	+	+	x	x
Base utilizada por Eve	+	x	+	x
Base utilizada por Bob	+	+	x	x
Ocorrência na <i>sifted key</i>	25%	25%	25%	25%

Nos casos em que Eve faz medições nas mesmas bases que Alice e Bob, o resultado obtido por Bob não é alterado, porém, quando Eve introduz uma medição com uma base errada, os resultados das medições de Bob são aleatórios, portanto apenas metade dos resultados está correta. Com isso, tem-se que a taxa de erro da chave filtrada com a espionagem é de 25%, metade da segunda coluna e metade da terceira coluna da figura 8 (MARQUEZINO, 2003). Caso Alice e Bob obtenham uma taxa de erro tão alta, é interessante que eles abortem o protocolo (BRUSS *et al.*, 2007).

Há, também, uma versão do protocolo BB84 baseada em emaranhamento. Essa versão utiliza ideias do protocolo BB84 com conceitos de emaranhamento vistos no teletransporte quântico. Alice e Bob compartilham um número n estado de Bell:

$$|\Phi^+\rangle^{\otimes n} = |\Phi^+\rangle \otimes \dots \otimes |\Phi^+\rangle.$$

Com isso, sabe-se que os resultados das medidas de Alice e Bob estão correlacionados, e, como esses estados são puros, não é possível para Eve emaranhá-los com outros *qubits* (BRUSS *et al.*, 2007). O funcionamento deste protocolo, porém, não será aprofundado por não ser o foco deste artigo.

5 Fortalecimento Do Protocolo Bb84

O protocolo BB84 utiliza duas bases em todo o processo, a base retilínea com as polarizações em 0° ou 90° e a base diagonal com polarizações em 45° ou 135° . Se um intruso tentar interceptar a comunicação do protocolo BB84, em cada medição feita, o intruso terá uma probabilidade de 50% para acertar a base escolhida por Alice e obter uma parte da informação. Para minimizar a informação obtida pelo interceptador, o protocolo BB84 utiliza um passo de amplificação de privacidade, contudo esse processo não é capaz de reduzir a zero a informação obtida por Eve.

A ideia principal deste trabalho é minimizar a informação que um intruso consegue extrair ao observar o canal quântico, sem a necessidade de enviar uma quantidade maior de *qubits*, aumentando, assim, a segurança do protocolo. Primeiro será explicada a proposta de fortalecimento, depois serão mostrados os cálculos que levaram às decisões. No decorrer da explicação serão feitas comparações da proposta com o protocolo BB84 e serão apresentados alguns exemplos.

A proposta para o fortalecimento do protocolo BB84, é a inclusão de duas novas bases para a polarização e medição dos fótons sem diminuir a informação obtida por Bob. Para isso, será utilizada uma estratégia na polarização e medição dos fótons.

A estratégia adotada consiste em usar chaves cíclicas, compostas por seis pares formados pelas quatro bases. Esta chave deve ser compartilhada antes do início do protocolo, como verificador, para evitar que Eve tente se passar por Alice ou Bob e estabeleça uma comunicação falsa.

O início do fortalecimento do protocolo BB84 é semelhante, em parte, ao protocolo original, no qual Alice escolhe aleatoriamente uma sequência de *bits* que, no caso do fortalecimento, deverá ser um conjunto de seis pares, ou múltiplos de seis, isso será melhor detalhado ao longo do texto. Em seguida, Alice polarizará os fótons de acordo com o valor do *bit*. Para isso, Alice deve utilizar a sua chave cíclica compartilhada com Bob e, seguindo a ordem da

chave, ela deverá escolher aleatoriamente uma das duas bases de cada par e enviar o fóton a Bob.

Para Bob realizar as medições, ele também deverá utilizar a chave cíclica. Da mesma forma que Alice, Bob irá escolher uma entre as duas bases de cada par da chave cíclica, respeitando a ordem. Como Alice e Bob possuem as mesmas chaves cíclicas a probabilidade de Bob acertar uma medição é de 50%, a mesma proporção oferecida pelo protocolo BB84. Mas, para um intruso, as chances de interceptar uma informação com quatro bases é de 25%, ao contrário do BB84, que fornece 50%.

Após Bob realizar as medições, ele anuncia para Alice, por meio de um canal clássico, as bases que escolheu para medir os *qubits*, e Alice envia para Bob as bases utilizadas para polarizar os fótons. Ambos irão descartar as bases divergentes e, com as bases corretas, formarão a chave filtrada que, a princípio, deverá ser a mesma para ambos, considerando um canal sem ruído.

Com a chave filtrada, Alice e Bob compartilham parte da chave para verificar se houve interceptação na comunicação, calculando a taxa de erro no subconjunto da chave filtrada. Outra vantagem do fortalecimento é tornar o canal mais sensível a intrusos. No protocolo BB84, por exemplo, quando Eve intercepta todos os *qubits* e os reenvia para Bob, Eve introduz um ruído de 25% na chave filtrada, podendo, assim, ser detectado. Aplicando uma estratégia de interceptação, medindo apenas parte da informação, Eve pode não ser detectado e conseguir parte da informação. No fortalecimento proposto, entretanto, se Eve interceptar toda a comunicação o ruído introduzido será de 37,5%, o que obriga Eve a interceptar menos informações que no protocolo BB84 para não ser detectado.

A correção de erros, em caso de um canal com ruídos, e a amplificação de privacidade são realizados da mesma maneira que o protocolo BB84.

Na proposta, são adicionadas duas novas bases ao protocolo BB84, as bases **M** e **N**, aplicadas em uma estratégia de chave cíclica. As bases **M** e **N** correspondem, às polarizações em 30 ou 120 graus e 60 ou 150 graus, respectivamente, como mostrado na Figura 7. Para facilitar a nomenclatura, a base retilínea será chamada de base **R** e a base diagonal será chamada de base **D**.

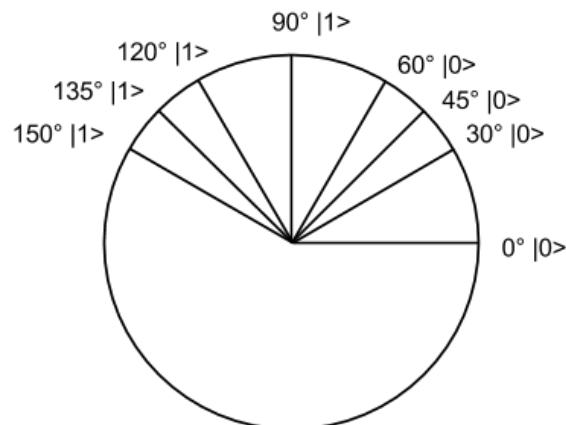


Figura 7: As quatro bases usadas no fortalecimento do protocolo BB84.

Simbolicamente:

- A base **R** representará os eixos de 0° e 90° ;
- A base **M** representará os eixos de 30° e 120° ;
- A base **D** representará os eixos de 45° e 135° ;
- A base **N** representará os eixos de 60° e 150° .

Abaixo será descrito como aplicar o fortalecimento ao protocolo sem prejudicar a quantidade de informação que Bob consegue medir no protocolo BB84 nem a quantidade de *qubits* que trafegam no canal quântico.

Para iniciar o protocolo BB84, Alice e Bob devem ter conhecimento de uma chave secreta, compartilhada previamente, para evitar que Eve tente se passar por um dos dois. No fortalecimento do protocolo BB84, esta chave secreta deverá ser uma sequência de pares aleatórios, formados pelas quatro bases descritas acima, e o comprimento da chave é calculado e padronizado para garantir maior segurança.

O tamanho mínimo da chave deve ser de seis pares e deve crescer aritmeticamente com razão seis. A quantidade mínima de pares da chave foi calculado de acordo com o número mínimo de comutações das quatro bases, sem privilegiar nenhuma, evitando uma perda maior de informação para Eve, como mostram os cálculos abaixo:

- Há quatro bases diferentes, **R**, **D**, **M** e **N**;
- Deve-se formar a maior sequência de pares possíveis, sem repetição;

Aplicando a fórmula de combinação simples de análise combinatória:

$$\frac{n!}{k!(n-k)!} = \frac{4!}{2!2!} = 6.$$

Onde **n** é o número de elementos diferentes e **k** é a quantidade de elementos em cada subconjunto, no caso **k** = 2, pois são pares de bases. Este resultado representa o número de pares diferentes que compõem uma chave. Resultando em seis combinações possíveis de pares de quatro bases distintas, sem repetição:

$$RD, NM, RN, DM, RM, DN.$$

As seis variáveis da chave resultam em 6! combinações, ou seja, 720 chaves diferentes. A probabilidade de Eve acertar aleatoriamente a sequência de uma chave de seis pares é de $1/6! = 0,139\%$ para acertar a chave inteira e conseguir medir 50% da informação, ou $1/(6*5*4) = 0,83\%$ de acertar metade da chave e conseguir medir 25% da informação. Portanto, não é interessante para Eve tentar adivinhar a chave pelo desconhecimento do tamanho da chave e porque para cada aumento de seis posições na chave há uma diminuição de cinco casas decimais na probabilidade de Eve acertá-la, como ilustrado no exemplo a seguir :

- A probabilidade de acertar uma chave com seis pares é:
chave {RD, NM, RN, DM, RM, DN}

$$1/6 * 1/5 * 1/4 * 1/3 * 1/2 * 1 = (1/6!)^1 = 0,139\%;$$

- A probabilidade de acertar uma chave com doze pares é:

chave {RD, NM, RN, DM, RM, DN, RD, NM, RN, DM, RM, DN}

$$\begin{aligned} 1/6 * 1/6 * 1/5 * 1/5 * 1/4 * 1/4 * 1/3 * 1/3 * 1/2 * 1/2 * 1 * 1 = \\ = 1/6! * 1/6! = (1/6!)^2 = 0,193 * 10^{-7} = 0,193 * 10^{-5}\%. \end{aligned}$$

- A probabilidade de Eve acertar uma chave diminui exponencialmente:

$$(1/6!)^n,$$

onde o aumento de n significa aumentar a chave em $6n$ posições.

Com a inclusão das duas bases, a quantidade de informação que Eve consegue extrair do canal quântico cai de 50% para 25%, ou seja, a quantidade de informação que Eve conseguiria obter no protocolo BB84 é reduzida pela metade com a introdução dessas duas novas bases.

Se, ao invés de tentar descobrir a chave, Eve empregar uma estratégia na medição, como, por exemplo, utilizar apenas uma das bases para aumentar a quantidade de informação extraída, levando em conta que qualquer uma das quatro bases aparecem em metade dos pares da chave, Eve pode escolher uma única base para medir todos os *qubits*. Supondo R como a base escolhida, para cada *qubit* polarizado em um dos três pares RN, RD ou RM, em uma chave de qualquer tamanho ou ordenação, Eve terá 50% de acerto em 50% das medições, o que resulta em 25% da informação, como mostrado na tabela 3. A mudança de estratégia rendeu a Eve 25% da informação, porém, se compararmos ao protocolo BB84, que fornece 50% da informação, esta estratégia melhora em 50% a segurança do protocolo.

Tabela 3: Comparação dos dados obtidos por Eve no protocolo BB84 e no fortalecimento proposto

<i>Bits aleatórios de Alice</i>	1	1	0	1	0	0	0	0	1	1	0	1
<i>Chave inicial de tamanho 12</i>	RN	NM	RD	DM	RM	DN	RD	DN	RN	DM	RM	NM
<i>Base escolhida por Alice no fortalecimento do protocolo BB84</i>	N	M	R	D	M	N	R	D	N	D	R	M
<i>Base escolhida por Alice no protocolo BB84</i>	R	D	R	D	D	D	R	R	R	D	R	D
<i>Base escolhida por Eve</i>	R	R	R	R	R	R	R	R	R	R	R	R
<i>Informação interceptada por Eve no fortalecimento do protocolo BB84</i>			0				0				0	
<i>Informação interceptada por Eve no protocolo BB84</i>	1		0				0	0	1		0	
<i>Informação protegida pelo reforço do protocolo BB84</i>	1						0	1				

Com Alice e Bob compartilhando a mesma chave, {RD, NM, RN, DM, RM, DN}, pode-se dar início ao fortalecimento do protocolo BB84. Inicialmente, Alice escolhe aleatoriamente uma sequência de *bits*, da mesma forma que no protocolo BB84, porém a quantidade de *bits* deve

ser um múltiplo de 6. A diferença neste primeiro passo é a forma de escolher as bases para a

polarização dos *qubits*. Suponha que Alice escolheu aleatoriamente a sequência de *bits* 010111001010. Alice, então, aplica a sua chave no início da sequência de *bits* e a repete até cobrir todos os *bits*, como ilustrado na Tabela 4.

Tabela 4: Montagem da chave cíclica

<i>Bits de Alice</i>	0	1	0	1	1	1	0	0	1	0	1	0
<i>Chave compartilhada</i>	RD	NM	RN	DM	RM	DN						
<i>Aplicar a chave até o fim da sequência</i>							RD	NM	RN	DM	RM	DN

Seguindo o padrão do protocolo BB84, Alice irá escolher aleatoriamente uma entre as duas bases, de acordo com a sequência da chave pré-estabelecida, e enviará a Bob os fótons polarizados, como mostra a Tabela 5.

Tabela 5: Utilização da chave cíclica para a polarização dos fótons

<i>Bits de Alice</i>	0	1	0	1	1	1	0	0	1	0	1	0
<i>Chave cíclica</i>	RD	NM	RN	DM	RM	DN	RD	NM	RN	DM	RM	DN
<i>Base escolhida por Alice aleatoriamente baseado no par da chave</i>												
<i>Polarização dos fótons</i>	R	M	N	D	M	N	R	M	N	D	R	D
	0°	120°	60°	135°	120°	150°	0°	30°	150°	45°	90°	45°

Bob, por sua vez, utilizará o mesmo método de Alice para fazer as medições. Aplicando a sua chave cíclica, ele escolhe aleatoriamente qual das duas bases será utilizada. Em seguida, Bob anuncia para Alice as bases que foram utilizadas para fazer as medições e Alice envia para Bob quais bases foram utilizadas para polarizar cada fóton. Com isso, ambos terão a mesma sequência de *bits*, que compõe a chave filtrada, caso não haja interceptação na comunicação e o canal seja um canal quântico ideal, como demonstrado na Tabela 6, próxima página.

Tabela 6: Utilização da chave cíclica para a medição dos fótons

<i>Bits de Alice</i>	0	1	0	1	1	1	0	0	1	0	1	0
<i>Base escolhida por Alice aleatoriamente</i>	R	M	N	D	M	N	R	M	N	D	R	D
<i>Base escolhida por Bob aleatoriamente</i>	R	M	M	D	N	D	D	M	N	N	R	R
<i>Bits obtidos pelas medições de Bob</i>	0	1		1				0	1		1	

No fortalecimento, assim como no protocolo BB84, após Alice e Bob criarem a chave filtrada, é aplicado o passo de verificação de erro para detectar se houve interceptação de informação ou não, dando continuidade ao protocolo. Sem a presença de um intruso, a quantidade de informação da chave filtrada deve refletir em 50% da chave bruta em um canal ideal. A figura 8 mostra que a informação de Bob estará correta apenas quando ele fizer as medições nas mesmas bases que Alice. A chave cíclica direciona Bob a medições mais precisas, dando duas opções de bases para efetuar cada medida, o que equivale a 50% das medições em cada base, mantendo a mesma proporção que o protocolo BB84.

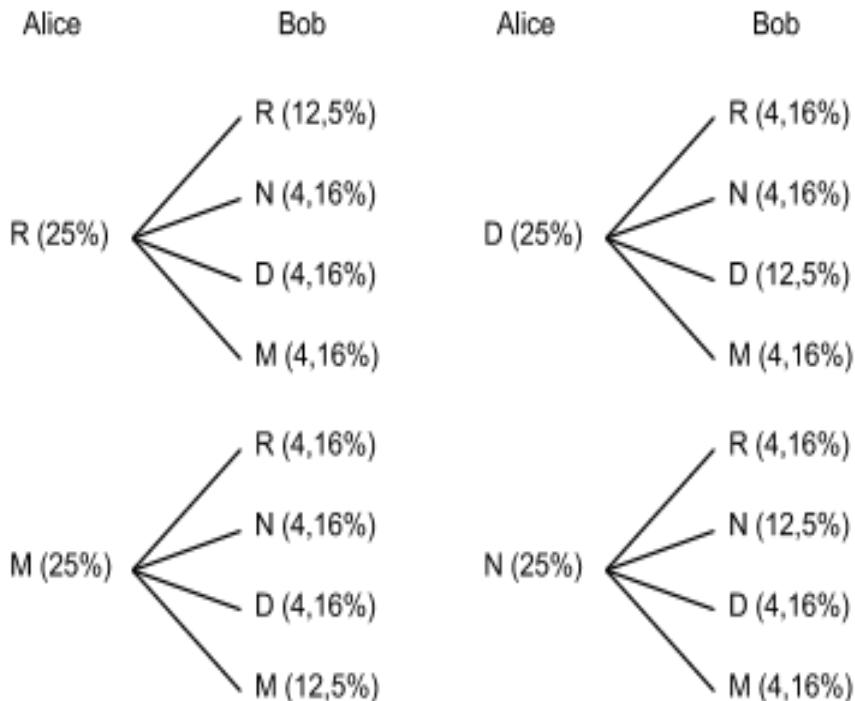


Figura 8: Casos possíveis sem interferências de um intruso.

Quando Eve intercepta toda a comunicação, interceptando e reenviando os *qubits* para Bob, Eve introduz um ruído de 25% na chave filtrada no protocolo BB84, podendo, assim, ser detectado. Com o fortalecimento, se Eve utilizar o mesmo método de interceptação e reenvio, a diferença entre as chaves filtradas sobe para 37,5% e, com um ruído maior, torna-se mais evidente a sua intrusão na comunicação. Como Eve não sabe em qual base medir, ele terá que escolher uma base entre quatro, enquanto Bob escolhe uma entre duas. Isso diminui as chances de Eve de acertar uma medição ao repassar a Bob, que antes era de 50% e agora é 25%.

Pelo fato de a chave cíclica compartilhada entre Alice e Bob antes do início do protocolo ser composta por quantidades iguais de cada base, a probabilidade de Bob medir cada base é a mesma. Ou seja, de todos os fótons polarizados por Alice, metade serão medidos pelas bases corretas e as outras serão medidas pela outra base do par na chave cíclica de Bob. Como Eve não tem conhecimento da chave cíclica, ele terá que medir aleatoriamente em uma das

quatro bases dividindo a probabilidade de cada base em quatro e distorcendo as medições de Bob, como mostra o esquema da figura 9:

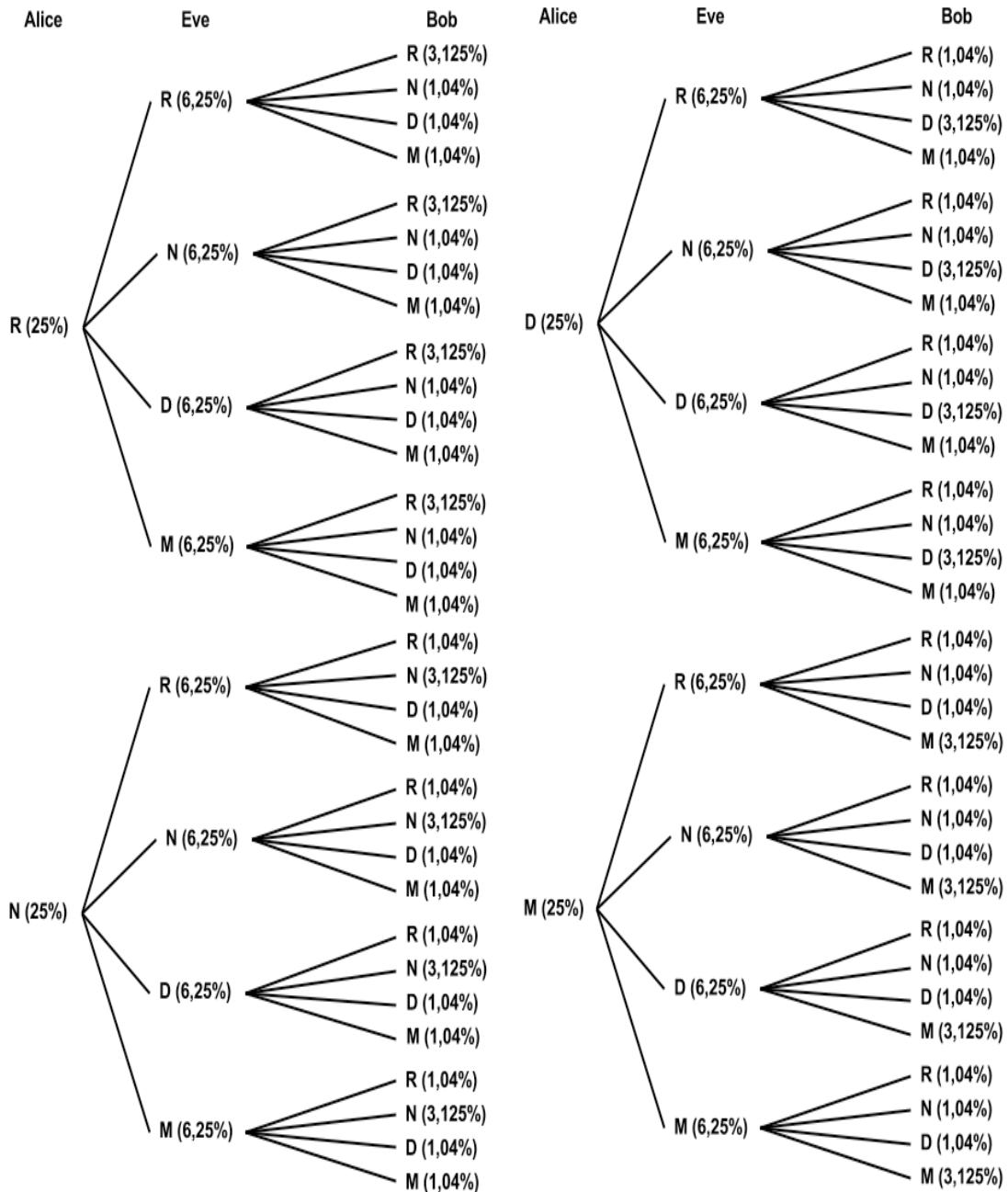


Figura 9: Casos possíveis com a interferência de um intruso.

As medições de Bob, seguindo a chave cíclica, correspondem a 50% nas bases corretas e os outros 50% serão distribuídos nas demais bases. Com a interceptação de Eve, os resultados das medições de Bob dependem das bases que Eve utilizou para medir os *qubits* antes de reenviá-los para Bob, lembrando que, quando Eve introduzir uma base errada e reenviar o *qubit* para Bob, suas medições tornam-se aleatórias, corrompendo metade dessas medições.

A Tabela 7 representa a análise do resultado da chave filtrada, indicando a quantidade de informação que Bob terá com a intrusão de Eve. Para cada base errada que Eve utilizar, Bob terá uma redução de metade da informação correta daquela base, e para cada base correta que Eve utilizar Bob não terá seu resultado alterado.

Tabela 7: Análise da chave filtrada

Base de Alice	R	R	R	R	N	N	N	N	D	D	D	D	M	M	M	M
Base de Eve	R	N	D	M	R	N	D	M	R	N	D	M	R	N	D	M
Base de Bob	R	R	R	R	N	N	N	N	D	D	D	D	M	M	M	M
Chave Filtrada (%)	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25
Informação correta de Bob (%)	6,25	3,125	3,125	3,125	3,125	6,25	3,125	3,125	3,125	3,125	6,25	3,125	3,125	3,125	3,125	6,25
Informação roubadas por Eve	6,25					6,25					6,25					6,25

Desta forma, é possível calcular a taxa de erro da chave filtrada da seguinte forma:

Informação que Eve utilizou a base correta:

$$4 * 6,25 = 25\%.$$

Informação que Eve utilizou uma base incorreta, reduzindo a informação de Bob:

$$12 * 3,125 = 37,5\%.$$

Observando que a informação que Bob perdeu, não é a informação que Eve ganhou. Sendo assim, a interceptação de Eve introduziu no sistema uma taxa de erro de 37,5%, entretanto, em um canal ideal não deveria haver erros. Neste caso, o procedimento é o mesmo do protocolo BB84, interromper a comunicação e voltar para o início do fortalecimento do protocolo BB84.

Caso não seja detectada a presença de nenhum intruso na comunicação de Alice e Bob, no fortalecimento do protocolo, os passos seguintes são os mesmos do protocolo BB84, correção de erros usando o canal clássico e amplificação de privacidade, para reduzir ainda mais a informação obtida por Eve.

6 Conclusões E Trabalhos Futuros

Este artigo definiu conceitos importantes sobre computação quântica e informação quântica para explicar o funcionamento do protocolo BB84 e sugerir uma forma de fortalecê-lo. O fortalecimento propôs a adição de duas bases além das já existentes para diminuir a informação adquirida por um possível intruso, porém sem comprometer a informação obtida pelo receptor. Cálculos mostram que o método de fortalecimento manteve a porcentagem de informação obtida pelo receptor e aumentou a taxa de erros introduzidos pelo interceptador,

o que, consequentemente, reduz a quantidade de informação que o intruso pode adquirir sem ser detectado pelo protocolo.

Este trabalho tem uma contribuição não só no aumento da segurança do protocolo, que é um dos protocolos de distribuição de chaves quântica mais estudados, mas também no desenvolvimento desta área, ainda pouco trabalhada.

Por ser uma área pouco trabalhada, uma das dificuldades encontradas neste trabalho foi a baixa quantidade de materiais atualizados referentes ao assunto de mecânica quântica e sobre a linguagem de programação quântica QCL (do inglês, *Quantum Computing Language*), se comparados com mecânica clássica e uma linguagem de programação clássica como Java.

Como trabalhos futuros, tem-se a opção de desenvolver um algoritmo do fortalecimento do protocolo BB84, na linguagem QCL (do inglês, *Quantum Computer Language*), e analisar o seu comportamento e desempenho comparado ao protocolo BB84 sem o fortalecimento, com o intuito de adicionar e promover alternativas no ramo da criptografia quântica, e, assim, expandir as opções de protocolos para garantir a segurança da informação na computação quântica, tanto utilizada em fibra ótica, quanto em computadores quânticos, quando forem desenvolvidos.

Outra possibilidade de um trabalho futuro seria o estudo mais aprofundado dos protocolos de distribuição de chave, buscando outra forma de melhorar outros protocolos existentes ou de desenvolver um novo protocolo, mais seguro e eficiente, dando, assim, continuidade ao desenvolvimento e acrescentando material no ramo da computação quântica, para evitar que a segurança da informação quântica seja comprometida com a quebra de um protocolo.

Referências Bibliográficas

BRUSS, D. et al. Quantum cryptography: a survey. Eletronic Colloquium on Computational Complexity, 2006.

FERNANDES, S. R. et al. Criptografia quântica, uma abordagem introdutória. XI Encontro de Modelagem Computacional, 2007.

GRIFFITHS, D. J. Introduction to quantum mechanics. Upper Saddle River: Pearson Prentice Hall, 2005.

KAYE, P. et al. An introduction to quantum computing. New York: Oxford University Press Inc., 2007.

MARQUEZINO, F. L. Estudo introdutório do protocolo quântico BB84 para troca segura de chaves. Revista Eletrônica de Iniciação Científica, 2004.

MCMAHON, D. Quantum computing explained. Hoboken: John Wiley & Sons, Inc., 2008.

CHRISTOFOLLETTI, T. V. D.; MELO, B. L. M. Computação quântica: estado de arte. Monografia, Santa Catarina: INE/UFSC, 2003.

NAKAHARA, M.; OHMI, T. Quantum computing: From linear algebra to physical realizations. Boca Raton: CRC Press, 2008.

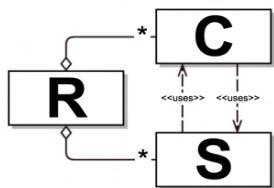
NIELSEN, M. A.; CHUANG, I. L. Quantum computation and quantum information. Cambridge: Cambridge University Press, 2010.

OLIVEIRA, A. G. Criptografia usando protocolos quânticos. Monografia, Lavras: Universidade Federal de Lavras, 2004.

PAPADAKOS, N. P. Quantum information theory and applications to quantum cryptography. Individual Study Option for the Department of Computing, Imperial College, UK. 2001.

STEANE, A. Quantum computing. Reports on Progress in Physics 61: p 117-173, 1997.

VENDRAL, V. Introduction to quantum information science. New York: Oxford University Press Inc., 2006.



Uma Análise sobre o Uso de Metáforas em Ambientes Virtuais de Ensino

Beatriz de Almeida Pacheco¹, Ilana A. Souza-Concilio¹, Eliani Maria Kfouri²

¹Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Rua da Consolação, 930 – São Paulo – SP - Brasil

²Mboé Educação em Rede
Rua Carapuri, 26 – São Paulo – SP - Brasil

{bia.pacheco, iasouza}@mackenzie.br, e.kfouri@mboeeducacao.com.br

Abstract. This article aims to discuss the use of visual metaphors in the development of interfaces of education at distance systems. An important tool used to achieve the goals of usability is the use of such artifices that exploit users' prior knowledge and repertoire to facilitate the communication process to define computational interactions difficult to articulate. In LMSs the use of this resource is generalized, which may end by emphasizing similarities, omitting important differences between the model used as a reference and the system that is drawn from it. In this sense, this paper presents the findings about the use of metaphors obtained from tests carried out by two groups of users of virtual learning systems: students and teachers.

Resumo. Este artigo tem como objetivo discutir o uso de metáforas visuais no desenvolvimento de interfaces de sistemas de educação a distância. Uma ferramenta importante usada para atingir os objetivos de usabilidade é o uso de tais artifícios, que exploram o conhecimento prévio dos usuários e repertório para facilitar o processo de comunicação ao definir interações computacionais difíceis de articular. Em AVEAS seu uso é generalizado, o que pode acabar por enfatizar semelhanças, omitindo importantes diferenças entre o modelo usado como referência e o sistema que é desenhado a partir dele. Neste sentido, o presente trabalho apresenta as conclusões obtidas a partir de testes sobre o uso de metáforas realizados por dois grupos de usuários de sistemas virtuais de aprendizagem: estudantes e professores.

1. Introdução

Para aprimorar a educação formal a distância foram desenvolvidos sistemas chamados *Learning Management Systems*, ou Ambientes virtuais de Ensino e Aprendizagem (*LMS* – AVEAS em português), que são aplicações de softwares ou tecnologias baseadas em

Web utilizadas para planejar, implementar e avaliar um processo de aprendizagem específica. Normalmente, um sistema dessa natureza possui um instrutor (ou professor) que cria e distribui conteúdo, e comumente monitora a participação dos alunos e avalia seu desempenho. O AVEAS também pode proporcionar aos alunos a possibilidade de usar recursos interativos, como fóruns de discussão e chats. Em tais ambientes há cada vez um número maior de ferramentas disponíveis para promover um processo rico de ensino e aprendizagem.

De acordo com Levy (2003), novas mídias e seus suportes suscitam novos e diferentes tipos de conhecimento. Assim, por meio da experimentação em interfaces e dispositivos interativos, as pessoas passam a aprender de maneiras distintas, o que acaba por afastar as tecnologias e estratégias de ensino tradicional da nova realidade do aluno, construída a partir dessas novas relações.

Neste sentido, as interfaces devem ser projetadas visando as necessidades e expectativas dos utilizadores, permitindo-lhes direcionar sua atenção para os objetos com os quais trabalham diretamente, de uma forma rápida, eficaz, eficiente e satisfatória, o que significa que o projeto deve ser centrado no usuário [Roberts et. al, 1998].

Assim, com a finalidade de se aproximar do universo do usuário, o uso de metáforas visuais (ícones, gráficos, disposição dos elementos visuais na interface) pode explorar o conhecimento prévio dos usuários e seu repertório para facilitar o processo de comunicação, aproveitando o conhecimento já consolidado e transformando a aprendizagem mecânica em significativa [Ausubel, 1968]. Assim, portanto, permite a definição de interações computacionais geralmente difíceis de serem articuladas.

As metáforas permitem compreender e experimentar um tipo de coisa em termos de outra, recurso que é amplamente utilizado na vida cotidiana. Elas também podem ser usadas no projeto de interfaces digitais para alavancar o conhecimento prévio dos usuários e definir interações computacionais difíceis de articular [Preece, Rogers and Sharp, 2005].

No entanto, o uso inadequado da metáfora, bem como de outras figuras de linguagem, pode dificultar ou mesmo impedir algumas ações interativas. As metáforas enfatizam semelhanças entre duas coisas, mas também podem omitir diferenças [Lakoff and Johnson, 1980] [Blackwell, 2006]. Se o uso de figuras de expressão não é cuidadosamente feito, o usuário pode ser levado a crer que o sistema tem alguns atributos que certamente não possui.

Este artigo é parte de uma investigação anterior, que propôs uma análise das metáforas visuais utilizados pelo AVEA Moodle, com base na pesquisa e na classificação proposta por Lakoff e Johnson (1980). Sua intenção é analisar essas metáforas a partir de impressões do usuário e de sua percepção. Nesse sentido foram analisados professores e alunos. Eles foram divididos em dois grupos, aqueles que já estavam familiarizados com o Moodle, e aqueles que nunca haviam interagido com o LMS analisado. Como metodologia de ensaio, utilizou-se a proposta de Nielsen (2000), com um número limitado de usuários.

F2. As metáforas: características e classificações

A partir da publicação de “Metaphors we live by”, por Lakoff e Jonhson (1980), diversos investigadores passaram a defender a ideia de que metaforizar processos é

característica inerente ao ser humano, fenômeno constituinte da cognição e linguagem humana. Para eles, a linguagem é inherentemente metafórica e presente desde as linguagens mais poéticas às mais rigorosas, como a linguagem científica.

O termo metáfora usado no design de interface é um pouco diferente do mesmo termo usado na literatura. Na literatura significa "uma comparação implícita entre duas coisas ao contrário de natureza que ainda têm algo em comum" [Corbett and Connors, 1999]. A importância da metáfora está em fazer um novo sistema se parecer e agir como um sistema já conhecido: metáforas de interface dão ao usuário um modelo a ser seguido, sem que haja necessidade que ele crie o seu.

No entanto, mesmo neste ambiente, deve-se atentar ao fato que o significado almejado pelo designer por meio de uma construção metafórica pode não ser entendida e estabelecida pelo usuário, uma vez que os elementos envolvidos na origem e destino decorrem de experiências pessoais. Contudo, este aspecto depende do tipo da metáfora produzida. As metáforas mais convencionais costumam aproximar de forma mais natural os processos de produção e compreensão, o que acaba por tornar menos importante o contexto e situação na construção de sentido [Gibbs, 1994; 2002].

Lakoff e Johnson (1980) explicam que as metáforas estão infiltradas na vida cotidiana, não somente na linguagem, mas no pensamento e na ação. Isso significa que os conceitos que estruturam os pensamentos orientam também o modo como as pessoas percebem, se comportam e se relacionam no mundo: de acordo com sua experiência física e cultural.

Existem várias classificações para metáforas. Por exemplo, elas podem ser classificadas de acordo com os termos linguísticos, de acordo com as relações envolvidas na associação, no que diz respeito ao tempo de sua adoção, entre outros.

Entre as classificações estudadas, algumas foram identificadas como apropriadas para Web. Destas, duas se destacam: uma é classificar metáforas de acordo com o tipo de relação entre os dois elementos envolvidos na associação e a outra é de acordo com seu tempo de existência [Lakoff and Johnson, 1980] [McLaren, 2000].

1. A classificação como função do relacionamento: este tipo de classificação envolve metáforas que relacionam uma coisa a outra. As relações envolvidas podem levar a:

- A. Metáforas estruturais: são usados para comparar um conceito a conceitos cotidianos [McLaren, 2000]. Eles caracterizam o conceito de estrutura em comparação com a estrutura de um outro processo [Lakoff and Johnson, 1980].
- B. Metáforas Orientacionais: transmitem o conceito de orientação espacial (para cima, para baixo), ou seja, um conceito explicado em termos de espaço. Eles organizam todo um sistema de conceitos de uma forma para se tornar possível relacionar um conceito para uma relação espacial [Lakoff and Johnson, 1980].
- C. Metáforas ontológicas: relacionam conceitos em termos de categorias básicas da existência como objetos ou como substâncias. A compreensão das experiências em termos de objetos ou substâncias permite selecionar partes da experiência e tratá-las como entidades discretas ou substâncias de um tipo de uniforme [Lakoff and Johnson, 1980].

2. Classificação em função da Existência: relaciona-se com a forma como as pessoas recebem as metáforas relativas uma coisa a outra: envolve uma relação já conhecido e familiar ou traz uma nova concepção de relacionamento que mostra um novo conceito.

- A. Metáforas convencionais: são aqueles já utilizados intuitivamente pelas pessoas. No ambiente Web, ele pode ser considerado tradicional, que já existia como interfaces gráficas digitais antes da popularização da Internet.
- B. Novas metáforas: são aqueles ainda não utilizados intuitivamente pelas pessoas. Neste caso, a estrutura da metáfora deve ser previamente estabelecida [McLaren, 2000].

4. Usabilidade: Conceitos e Testes

Atualmente, com o surgimento dos games, smartphones e outros dispositivos, usuários passaram a esperar algo mais agradável e intuitivo em interfaces, o que os torna mais críticos em relação aos produtos de operação complicada [Farias, 2002].

Usabilidade visa o desenvolvimento de interfaces que permitem a interação fácil, agradável, eficaz e eficiente. Deve permitir a criação de interfaces transparentes de modo a não dificultar o processo, permitindo o controle total do ambiente do usuário sem recorrer a um obstáculo durante a interação [Nielsen and Loranger, 2003] [Nielsen, 1993].

A forma mais comum de avaliar a capacidade de utilização de um sistema é a partir do acompanhamento da interação do usuário. Isto pode ser feito em um laboratório com uma quantidade representativa de utilizadores para os quais o sistema foi desenvolvido ou no ambiente de trabalho, onde o sistema vai ser implantado.

De acordo com Nielsen (1993) é possível, a partir de testes realizados com apenas cinco usuários, identificar a maioria dos problemas de usabilidade de um sistema. De acordo com o autor, quando o primeiro usuário é testado, cerca de um terço dos problemas de projeto e de usabilidade já podem ser resolvidos. A partir do segundo usuário testado, muitos dos problemas apontados pelo primeiro são percebidos novamente, e alguns outros são identificados. Esta série novas percepções vai diminuindo rapidamente, e, a partir do sexto usuário dificilmente alguma coisa nova e importante é detectada.

Nielsen (2000), afirma que com 5 usuários sendo testados, é possível identificar cerca de 85% dos problemas, e “distribuir seu orçamento para testes com usuários em vários pequenos testes em vez de despender tudo em um único estudo”. Portanto, não há nenhuma necessidade real de se fazer testes com muitos usuários, após o quinto usuário, “você está desperdiçando seu tempo observando os mesmos resultados repetidamente, mas não está aprendendo muita coisa nova” [Nielsen, 2000].

5. Metáforas em AVEAs: O Caso Moodle

Em ambientes virtuais de ensino e aprendizagem o uso de metáforas também é generalizado. Nesses espaços, a principal função desses elementos é de facilitar a navegação do aluno e do professor, possibilitando o acesso, interação e edição de conteúdo de forma interativa e imediata.

Para analisar o uso de metáforas em tais ambientes, esta pesquisa considerou o AVEA Moodle, plataforma desenvolvida colaborativamente e de distribuição gratuita. Devido

a sua natureza, muitos desenvolvedores ao redor do mundo criam seus próprios temas (interfaces gráficas), que tendem a usar elementos visuais de bibliotecas existentes ou a desenvolver sua própria família de elementos gráficos. De um jeito ou de outro, muitos deles começam a partir de associações comumente vistas nas interfaces do sistema operacional Linux, que é projetado de forma semelhante ao LMS em questão [Pacheco and Kfouri, 2012].

Para analisar os elementos de imagens metafóricas, foram analisados os ícones padrão da ferramenta e aqueles usados no skin da interface utilizada pela Instituição de Ensino Superior. Ícones pertencentes a todas as categorias apresentadas por Moknern (1997) e Lakoff e Johnson (1980) foram encontrados.

5.1. Análise de metáforas visuais de acordo com a percepção do usuário

Para a coleta de dados precisos, os usuários foram divididos em dois grupos: os que ainda não tiveram contato com a plataforma (01) e os que já tiveram contato com a plataforma (02). Além disso, eles foram também divididos em: alunos (A) e professores (P). Portanto, nas análise aparecerão notações do tipo: P01, P02 ou A01 e A02. A eficiência das metáforas visuais foi testada a partir de um questionário on-line respondido por eles.

Os grupos de estudantes são os que interessam mais a pesquisa pois, como apontado no presente estudo, uma interface de interação que proporciona comandos intuitivos e transparentes proporciona a possibilidade de aumento de gasto de energia do aluno no processo de ensino e aprendizagem (conteúdo a ser aprendido), objetivo primeiro de sua interação.

Este questionário tem quatro grupos de questões: perfil do usuário, perguntas abertas, em que o usuário deve associar as imagens apresentadas a um conceito (área de ação / tarefa / aplicação), questões de múltipla escolha em que os usuários devem associar a imagem apresentada um dos conceitos fornecidos, e associações livres em que o usuário deve associar uma imagem (em sua cabeça) aos conceitos apresentados.

Quinze (15) estudantes e cinco (5) professores de cada grupo foram testados com base na metodologia de Nielsen (2000).

5.2. Análise dos resultados

Grupo de Alunos:

O grupo A01 é composto por 15 estudantes universitários que, apesar de usar um LMS na instituição em que estudam, este não é Moodle. Dessa forma eles não estão familiarizados com as metáforas visuais apresentadas. Este grupo apresenta um equilíbrio de gênero (8 mulheres e 7 homens) e de idade (87% entre 18 e 25 anos).

Já o grupo A02 é formado por estudantes predominantemente jovens (67% tem entre 18 e 25 anos) que utilizam o Moodle diariamente. Vale a pena destacar o pequeno número de mulheres pesquisadas nesse grupo pelo fato destes pertencerem à cursos ligados à tecnologia (apenas uma).

A seguir são destacadas algumas respostas emblemáticas da pesquisa. Os primeiros exemplos foram colhidos a partir do grupo de questões abertas.

Uma das imagens mostradas aos usuários foi a que representava “meus arquivos privados” (Figura 01a). Embora não houvessem suposto corretamente o nome da área no AVEA, 73% da primeira amostra (grupo A01) fez a associação adequada. Já no Grupo A02, formado por usuários do sistema, surpreendentemente nenhum deles foi capaz de associar o ícone que representa a sua área de trabalho cotidiano (“meus arquivos privados”), mas 86% fizeram uma associação correta com a ideia do que ele representava.



Figura 01. Ícones: (a) “Meus arquivos privados”; (b) Calendário

A imagem representada na Figura 01b, Calendário, por sua vez, refere-se a uma representação comum em interfaces digitais. Neste caso, 100% das associações feitas pelo grupo A01 foram próximas da função do ícone, e, dentre elas, 66% usaram exatamente a denominação usada no AVEA.

Já no grupo A02, todos os alunos fizeram associações apropriadas e 93% fizeram exatamente a associação proposta pelo Moodle da Universidade em que estudam.

Uma outra associação que mostrou resultados interessantes foi a que dizia respeito ao Glossário do Moodle. Uma metáfora que expressa uma área típica nos ambientes virtuais de ensino e aprendizagem e que costuma estar presente na maioria das interfaces, foi apontada por apenas um dos alunos analisados no grupo A01, enquanto apesar de usarem a interface diariamente, apenas dois alunos do segundo grupo fizeram a associação esperada.

Outro resultado semelhante ocorreu quando foi analisado o ícone que representava “meus cursos” no AVEA (Figura 02). Nenhum dos alunos do grupo A01 foram capazes de fazer associações apropriadas. Em contraste, 53% fez uma mesma associação errada, o que prejudica a compreensão da interface. Já no grupo A02, apenas um dos entrevistados foi capaz de fazer uma associação apropriada.



Figura 02. Meus cursos

No grupo de múltipla escolha pode-se destacar o resultado para o ícone “editar” (Figura 03a). Do primeiro grupo de usuários, 66% dos fez associação correta, enquanto no segundo grupo esse número caiu para apenas 40%, apesar do fato desses alunos lidarem diariamente com a metáfora.



Figura 03. Ícones para (a) “editar”; (b) “lição” e (c) “área ativa”

O segundo elemento refere-se aos trabalhos apresentados, lições (Figura 03b). Note que o nome e a divisão das atividades na plataforma, na versão em Português, muitas vezes faz com que haja alguns mal-entendidos, pois as palavras tarefas e lição costumam ser usadas como sinônimos. Assim, pela familiaridade com a plataforma, o número de associações assertivas aumenta significativamente, 40% no grupo A02 contra 6% no grupo A01.

Sobre o ícone que representa “área ativa” (Figura 03c), para os alunos que não conhecem a plataforma o significado associado é o de ideia (80%). No grupo A02, apesar do contato próximo, nenhum aluno indicou “área ativa” enquanto 66% também fez associação à ideia, como no primeiro grupo.

Finalmente sobre as questões associativas, quando a palavra solicitada foi “mensagem”, 73% dos entrevistados do primeiro grupo associaram a palavra a um envelope de carta e 20% a um balão de fala. Já no grupo A02, 100% dos entrevistados associaram a palavra com um envelope de carta, como no Moodle de sua Universidade.

Sobre o tópico “Edição”, 73% dos entrevistados do primeiro grupo fez a associação com um lápis, assim como os usuários do sistema, que fizeram a associação numa porcentagem semelhante (70%).

Já sobre “configurações”, destaca-se que 66% dos entrevistados associou a palavra com engrenagens no grupo A01 enquanto cerca de 80% do segundo grupo fez a mesma associação.

Grupo de Professores:

Foram testados dois grupos de professores com características semelhantes às dos alunos testados: não conhecedores/usuários do sistema (P01) e conhecedores/usuários do sistema (P02).

O grupo P01 foi composto por 05 professores universitários que usam um LMS na instituição em que trabalham, mas não é o Moodle. Assim, eles não estão acostumados com as metáforas visuais apresentadas. O grupo P02 consiste de professores da Instituição de Ensino Superior, familiares com a ferramenta.

Ambos os grupos são compostos por quatro homens e uma mulher; 70% dos entrevistados têm mais de 41 anos de idade, 20% têm entre 36 e 40 anos e 10% entre 31 e 35 anos.

Os mesmos testes realizados com os alunos também foram aplicados aos professores. Algumas respostas emblemáticas da pesquisa são destacadas a seguir. Os primeiros exemplos foram coletados do grupo de questões abertas.

Em relação à imagem que representa "meus arquivos privados" (Figura 01a), o primeiro grupo de usuários (P01), ao visualizar este ícone, fez uma associação com arquivo ou diretório; apenas um professor destacou a pasta pessoal. No grupo P02, formado por usuários do sistema, apenas um professor não fez a associação corretamente.

Já sobre a imagem que representa o calendário (Figura 01b), 80% das associações produzidas por ambos os grupos estavam corretas. Entre os professores que utilizam o

sistema e os demais testados que fizeram a associação correta, todos usaram exatamente a mesma nomenclatura usada pelo Moodle.

A associação que também mostrou resultados interessantes foi sobre o Glossário do Moodle. Uma metáfora que se refere a uma área típica de ambientes virtuais de ensino e aprendizagem e que é geralmente apresentada na maioria das interfaces, não foi nomeada por qualquer professor como era esperado.

Quanto ao ícone que representa "meus cursos" (Figura 02) no AVEA analisado, nenhum dos professores de ambos os grupos foi capaz de fazer a associação desejada pelos desenvolvedores.

É possível destacar o resultado para o ícone "editar" no grupo de múltiplas escolhas (Figura 03a). No primeiro grupo de usuários (P01), 80% fez a associação correta, enquanto que no segundo grupo (P02) este número desceu para apenas 60%, apesar do fato de estes professores lidarem diariamente com a metáfora.

No caso do elemento referente aos trabalhos apresentados em aulas, lições (Figura 03b), verificou-se que em ambos os grupos 40 % dos membros fez a associação correta.

Sobre o ícone que representa "área ativa" (Figura 03c), para usuários que não conhecem a plataforma, o significado associado foi o de ideia (100%). Já grupo P02, embora existisse o contato diário com a plataforma, apenas um professor indicou "área ativa", enquanto o restante relacionou a imagem com o conceito de ideia, como no primeiro grupo.

Finalmente, sobre as questões associativas, quando “mensagem” era a palavra solicitada, 100% dos entrevistados associaram a palavra ao envelope.

O lápis, por sua vez, foi a imagem indicada por quase todos os entrevistados quando perguntados sobre a função de edição. Apenas um professor, que não estava familiarizado com a interface, optou por um conjunto de ferramentas.

Sobre "configuração", destaca-se que todos os participantes do grupo P02 fez a associação desejada com engrenagens, enquanto as respostas do primeiro grupo (P01) foram variadas: sistemas, engrenagens de controle e pessoa.

Percebe-se, então, neste último grupo de questões, uma uniformidade maior nas respostas, o que indica a aproximação de significados das metáforas cujas ideias estão mais presentes nos Sistemas Digitais de um modo geral, sejam eles sistemas operacionais, interfaces web ou AVEAs.

Sobre alunos e professores: discussão

Como as metáforas, por muitas vezes, são utilizadas de maneira excessiva no desenvolvimento de sistemas interativos, alguns autores, como Donald Norman (1999) são céticos com relação ao seu uso. Para ele, o uso de metáfora é errado por definição uma vez que utilizá-las significa usar um objeto não necessariamente ligado ao propósito do sistema para que se estabeleça a relação. O autor defende a necessidade de se desenvolver um novo modelo conceitual compreensível que descreva os elementos constituintes da interface pelo que eles fazem e são. Segundo ele, a partir desse novo modelo, o usuário poderá aprender a interagir com a interface [Norman, 1999].

Nielsen e Loranger (2003), por sua vez, acreditam que metáforas podem ser usadas de forma cautelosa. Apesar dos autores acreditarem que muitas vezes é melhor desenvolver

um novo modelo conceitual, eles afirmam que seu uso traz benefícios, como o de facilitar o aprendizado dos usuários que poderão então usar um sistema com base em uma referência já familiar.

A partir da presente pesquisa teórica e dos resultados práticos obtidos por meio das análises dos testes realizados por professores e alunos, familiarizados ou não com a interface pesquisada, tende-se a concordar com a posição de Jakob Nielsen, que prega o uso cauteloso de tais associações.

Apesar das constatações de Lakoff e Johnson (1980) de que as metáforas estão infiltradas na vida cotidiana das pessoas, não somente em sua linguagem, mas pensamento e ação, quando se está diante de um sistema interativo tais associações podem variar muito conforme o repertório do usuário, e elementos projetados inicialmente para incrementar interações, podem acabar por comprometê-las. Ou seja, como já foi dito anteriormente, a experiência física e cultural, estão presentes e influenciam o modo como as pessoas percebem, se comportam e se relacionam no mundo.

Assim, deve-se atentar ao fato que o significado almejado pelo designer por meio de uma construção metafórica pode não ser entendida e estabelecida pelo usuário, uma vez que os elementos envolvidos na origem e destino decorrem de experiências pessoais [Gibbs, 1994; 2002].

A avaliação de metáforas com estudantes e professores mostrou que a familiaridade com o sistema realmente resolve alguns problemas associativos enquanto há o aprendizado de elementos visuais metafóricos. No entanto, esses elementos, se analisados fora do contexto de associação, podem resultar em associações truncadas ou incipientes. Nestes casos, percebe-se uma elevada sobrecarga cognitiva, o que sugere a utilização de texto complementar às metáforas ou ainda a substituição completa de tal recurso.

Assim, os resultados apresentados na presente pesquisa apontam para muitas dessas associações no ambiente Moodle serem equivocadas e não consoantes às experiências anteriores dos usuários analisados.

Ao se testar os usuários e se considerar suas experiências é possível preencher a lacuna existente em relação às motivações e necessidades das pessoas no processo de interação com sistemas e se propor metáforas que, de fato, possam auxiliar o processo interativo.

6. Considerações Finais

A análise revelou que, embora as metáforas possam fazer o usuário se sentir mais confortável em lidar com ideias e conceitos familiares, eles não determinam um objeto a se comportar exatamente como o outro. Durante a interação, o usuário terá que melhorar o padrão conceitual, porque o mais perto que eles podem ser o mundo da informática é diferente do real, por isso concluiu-se que as metáforas podem ser usadas, mas com cuidado e cautela.

Em termos cognitivos, os procedimentos analógicos dependem de conceitos mais concretos e mais perto da experiência dos usuários. Portanto, eles podem estender sua compreensão para níveis mais complexos e abstratos de conhecimento e apreensão da realidade. Este procedimento é altamente produtivo na ampliação e renovação do vocabulário de uma língua.

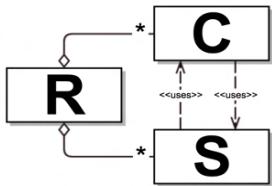
Embora tradicionalmente visto como um processo eminentemente semântico, ele realmente opera com regras pragmáticas. Se entendida apenas no nível semântico, a analogia metafórica pode não ser totalmente decodificada pelo receptor. As inferências não são dedutíveis de significados pragmáticos de regras lógicas, mas de regras de conversação, que são decorrentes das relações contextuais.

Como extensão desta pesquisa, pretende-se realizar outros testes em Ambientes Virtuais de Ensino e Aprendizagem com a finalidade de identificar um conjunto de metáforas que apresentem resultados ótimos em relação às relações que estabelecem com o que pretender ser ou fazer.

Referências Bibliográficas

- Ausubel, D.P. (1968). Educational psychology: a cognitive view. New York, Holt, Rinehart and Winston.
- Blackwell, A. F., 2006. The reification of metaphor as a design tool- ACM Transactions on Computer-Human Interaction (TOCHI) Vol.13, N.4, pg: 490–530.
- Corbett, Edward P. J., Connors, Roberts J., 1999. Classical Rhetoric for the Modern Student. New York, NY :Oxford University Press.
- Farias, Priscila (2002). Sign design, ou o design dos signos: a construção de diagramas dinâmicos para as classes de signos de C. S. Peirce. Tese de doutorado não publicada, Programa de Estudos Pós-Graduados em Comunicação e Semiótica, Pontifícia Universidade Católica de São Paulo.
- Gibbs, R. W., Jr. (2002).A new look at literal meaning in understanding what is said and implicated .Journal of Pragmatics, v.34, p.457-486.
- Gibbs, R. W., Jr.. (1994). The poetics of mind figurative thought language and understanding. Cambridge: Cambridge University Press.
- Lakoff, G.and Johnson, M., 1980. Metaphors we Live By. Chigago, IL:The University of Chicago Press.
- Levy, Pierre, 2003. A inteligência coletiva: por uma antropologia do ciberespaço. 4.ed. São Paulo, SP: Loyola.
- McLaren, Ian (2000). “Some pictorial symbol systems for public places”. In:Masoud Yazdani and Philip Barker (eds.) Iconic communication , pp. 42-50.Bristol: Intellect.
- Mokn kern, K., 1997. Visual Interaction Design: Beyond the Interface Metaphor – SIG- CHI Vol 29, n.2. Disponível em: <http://old.sigchi.org/bulletin/1997.2/vid.html#HDR3> Acesso em: 02/02/2012.
- Nielsen, J. (1993). Usability Engineering. San Francisco, CA: Morgan Kaufmann.
- Nielsen, J. and Loranger,H.,(2003). Prioritizing Web Usability. 1 Ed. Berkeley, CA: New Riders Press.
- Nielsen, J., 2000. Why You Only Need to Test with 5 Users. Disponível em <http://www.useit.com/alertbox/20000319.html>. Acesso em 14/03/2012.

- Norman, D.A. (1999). *The Invisible Computer: why good products can fall, the personal computer is so complex, and information appliances are the solution.* Massachusetts-The MIT Press.
- Pacheco, B. And Kfouri, E., (2012). Use of virtual metaphors in virtual environments: classification and uses. Proceedings of The International Conference on Innovations in Learning and Technology: Asia-Pacific Perspectives. University of Victoria, CA.
- Preece, J., Rogers, Y. and Sharp, H., 2005. *Design de Interação, além da Interação Homem- Computador*. São Paulo, SP: Bookman.
- Roberts, D., Berry, D., Isensee, S. and Mullaly J., 1998. *Designing for the user with OVID: Bridging User Interface Design and Software Engineering.* MacMillan Technical Publishing - Software Engineering Series.



Validação de um Modelo Computacional para o Controle de Tráfego Urbano

Luis Tadeu Mendes Raunheitte, Takato Kurihara, Rubens de Camargo, Arnaldo R. de Aguiar Vallim Filho, Júlio C. G. Petroni

Faculdade de Computação e Informática, Universidade Presbiteriana Mackenzie
raunheitte@mackenzie.br, takato@mackenzie.br, rcamargo@mackenzie.br,
arnaldo.aguiar@mackenzie.br, juliopetroni@yahoo.com.br

Abstract: *The purpose of this work is to present a computer model for the study of the urban car traffic jam. The model is a computer simulation using Matlab/Simulink to anticipate situations of a traffic jam. Several simulations were carried out and the model was considerably stable and reliable.*

Resumo. *O objetivo do trabalho é apresentar um modelo computacional para estudo do tráfego urbano de veículos. O modelo é simulado computacionalmente utilizando Matlab/Simulink para antecipar situações que levem a congestionamentos. Foram realizadas várias simulações e o modelo praticamente apresentou-se bastante estável e confiável.*

1. Introdução

A simulação computacional é a execução de um programa em computador com o objetivo de reproduzir um modelo abstrato de um sistema em particular, permitindo que sejam realizados estudos sobre estes sistemas de forma a tornar possível a avaliação do comportamento dos mesmos frente a variações no ambiente de estudo. De acordo com Freitas Filho [2008], o principal apelo ao uso da ferramenta de simulação computacional é a capacidade de responder questões sem que os sistemas investigados sofram qualquer perturbação.

Este trabalho apresenta um modelo computacional para o estudo do tráfego urbano, visando otimizar o fluxo de tráfego, reduzindo os congestionamentos, por meio de redução do tempo médio de espera dos veículos em filas de semáforos.

Apesar das potencialidades do uso da simulação no suporte à tomada de decisão, nas diversas áreas socioeconômicas, este trabalho emprega esta técnica na concepção de um modelo computacional para o estudo dos problemas relacionados ao tráfego urbano rodoviário, destacando-se nesse universo os problemas de fluidez.

Segundo Licínio da Silva Portugal [2005, p.105], diante da complexidade do sistema de tráfego, em particular o urbano, à medida que envolve inúmeras variáveis relacionadas tanto com a oferta quanto com a demanda viária, a técnica de simulação,

entre as diversas técnicas utilizadas, tem-se constituído uma importante ferramenta para auxiliar o trabalho do Engenheiro de Tráfego, permitindo apontar soluções para os vários problemas ligados ao trânsito. Problemas ligados ao trânsito urbano atingem milhões de pessoas todos os dias.

Considerando-se períodos críticos de congestionamento, pela manhã, a tarde e a noite, o custo relativo ao tempo ocioso despendido pelas pessoas no trânsito, o chamado “custo de oportunidade” [CAVALCANTI, 2008].

Além disso, pesquisas revelam que os congestionamentos acarretam também num maior consumo de combustível pelos automóveis, aumento da emissão de gases poluentes, como o CO₂. Outro fator que passou a ser considerado é o efeito psicológico que o tempo perdido acarreta no indivíduo e o que isso influencia na saúde e na qualidade de vida da população.

2. Modelagem e Simulação Computacional de Sistemas

Modelagem é a elaboração de um modelo para a representação de alguma coisa. Modelo é a representação de um sistema real ou imaginário usando uma linguagem.

Neste trabalho, a ferramenta utilizada para simulação é o *Simulink*, aplicativo para o ambiente *Matlab*, que fornece um ambiente interativo baseado em diagramas de blocos, voltado para modelagem, simulação e análise de sistemas dinâmicos contínuos, discretos ou híbridos [MATSUMOTO, 2003].

Os modelos são classificados, segundo Portugal [2005], em: estáticos e dinâmicos. Os dinâmicos, por sua vez, em determinístico e aleatórios. Os modelos aleatórios adotados neste trabalho são divididos em mudança discreta e contínua, conforme Figura 1.



Figura 1 – Classificação dos modelos de simulação. Fonte: Portugal [2005].

3. Tráfego Urbano

Na medida em que a aleatoriedade está intrínseca aos sistemas reais, especificamente na geração dos eventos desses sistemas que ocorrem ao acaso, a aplicação do método de Monte Carlo se faz necessária. A utilização dessa técnica consiste na geração artificial dos dados empregando-se um gerador de números aleatórios (GNA) e uma distribuição

de frequências da variável de interesse. O GNA é um programa computacional capaz de gerar valores aleatórios independentes e uniformemente distribuídos no intervalo de zero a um [FREITAS Filho, 2008].

O trabalho utiliza a nomenclatura proposta por Gucci [1996]. O termo trânsito é utilizado para tratar de deslocamentos de pessoas ou veículos e tráfego é aplicado quando se fizer relação com o estudo desses deslocamentos. O conceito de congestionamento está vinculado aos conceitos de capacidade da via e de nível de serviço. Enquanto a capacidade da via representa a quantidade máxima de veículos que pode se movimentar em um trecho em um intervalo de tempo, sob um conjunto especificado de condições de composição de demanda de tráfego e ambiente; o nível de serviço é uma medida de qualidade do serviço para o usuário da via.

Essa qualidade de serviço pode ser analisada sobre aspectos como frequência de paradas, velocidade de operação, tempo de viagem, densidade de tráfego e os custos operacionais do veículo. Ainda de acordo com o Gucci [1996], o nível de serviço é um parâmetro que retrata as condições de fluidez, segurança e conforto em um determinado espaço ocupado.

O volume de tráfego por hora em uma pista varia com a demanda e com a velocidade, que por sua vez, varia em função, por exemplo, do tipo de coordenação semafórica, da eficiência da fiscalização sobre o estacionamento proibido, ou ainda das condições topográficas. Além disso, ao longo do dia a demanda varia de acordo com os horários de maior movimento, e o congestionamento se apresenta quando o volume de tráfego supera a capacidade das vias [IPEA. 1997].

A fim de tornar o modelo mais próximo da realidade, quanto à demanda de utilização do sistema, tempos dos ciclos semafóricos e outros aspectos, este trabalho utiliza-se das definições do *Manual de Semáforos* do DENATRAN [1984]. Além disso, o cálculo dos tempos semafóricos é baseado no método de *Webster*, cujo algoritmo está descrito e definido em [DENATRAN, 1984].

4. Elaboração do Modelo Computacional

Este trabalho desenvolve um modelo de estudo de tráfego macroscópico, que visa à coordenação semafórica através de um controle isolado do cruzamento, utilizando-se uma programação de tempos fixos, e automática para o tempo de ciclo, duração e instantes de mudança [DENATRAN, 1984].

A figura 2, próxima página, ilustra o cruzamento que foi utilizado para o estudo, caracterizado por uma interseção entre duas vias de dupla mão de direção e cujo movimento é conflitante. A via A apresenta três faixas para tráfego e é composta pelas aproximações I e III, enquanto a via B apresenta apenas duas faixas e é composta pelas aproximações II e IV. Devido ao movimento conflitante entre as vias, os semáforos veiculares numerados de I a IV realizam o controle do tráfego alternando o direito de passagem no cruzamento.

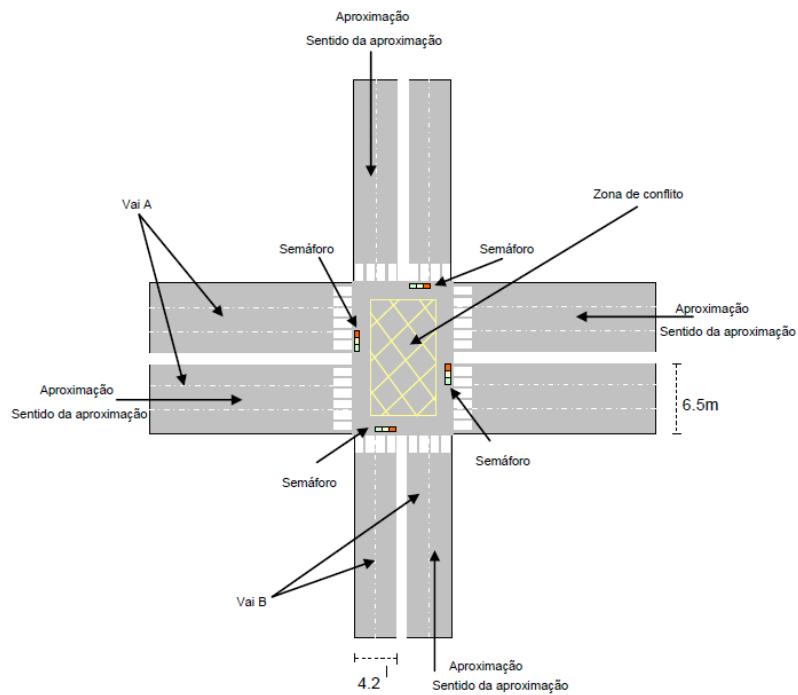


Figura 2 – Esquema do cruzamento estudado

O diagrama de estágios Denatran [1984] da Figura 3 representa esquematicamente a sequência de movimentos permitidos e proibidos para cada intervalo do ciclo em cada um dos estágios.

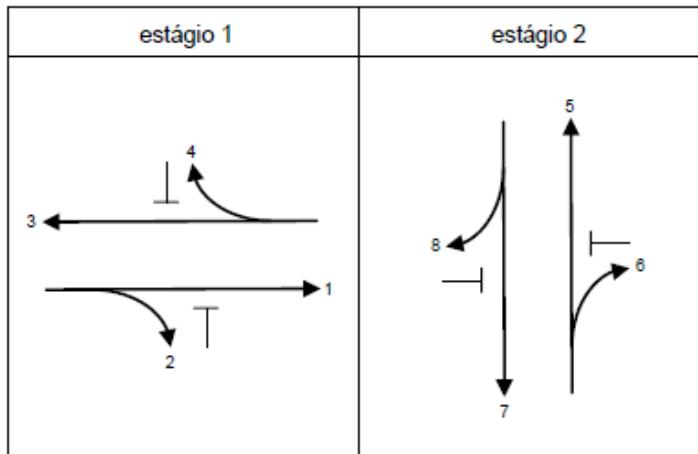


Figura 3 – Diagrama de estágios do cruzamento estudado.

5. Geração do sinal de controle do semáforo

A seguir apresenta-se o subsistema desenvolvido no Simulink para fornecer o sinal de controle da sequencia de sinalização para os semáforos do modelo. Cada estágio do ciclo de sinalização (ou seja, cada cor sinalizada: verde, amarelo e vermelho, nesta ordem) possui um valor de sinal discreto que será gerado de acordo com sua respectiva duração, a ser parametrizada no subsistema, conforme será descrito a seguir.

A Figura 4 apresenta um panorama geral do subsistema. Cada bloco foi numerado para facilitar a sua descrição:

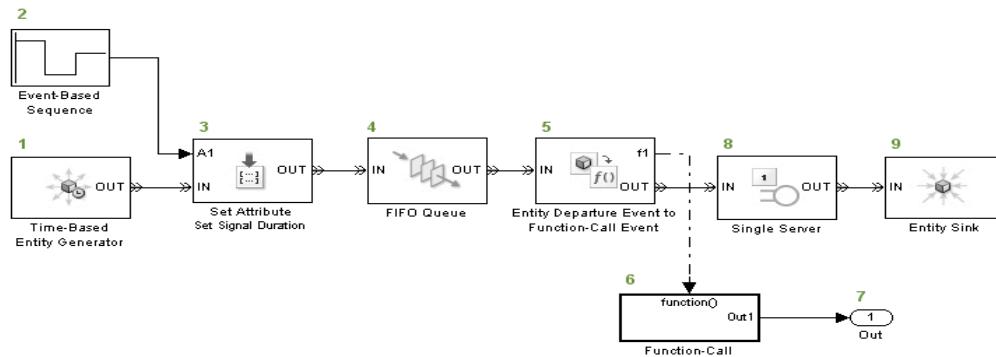


Figura 4 – Subsistema para geração do sinal de controle do semáforo.

1. Gera de forma sequencial o sinal de controle para cada estágio do semáforo no modelo. Cada estágio é representando como uma entidade gerada a um intervalo constante de um segundo. A rigor, este tempo de geração não importa, pois o controle da duração do sinal será realizado através do bloco sete, que será descrito adiante.
2. Gera um sinal cíclico com os valores que representam a duração dos estágios do semáforo. Este sinal cíclico é definido nas propriedades do bloco através de um vetor unidimensional formado pelos parâmetros do subsistema e que representam os valores para cada estágio do semáforo, conforme Figura 5:

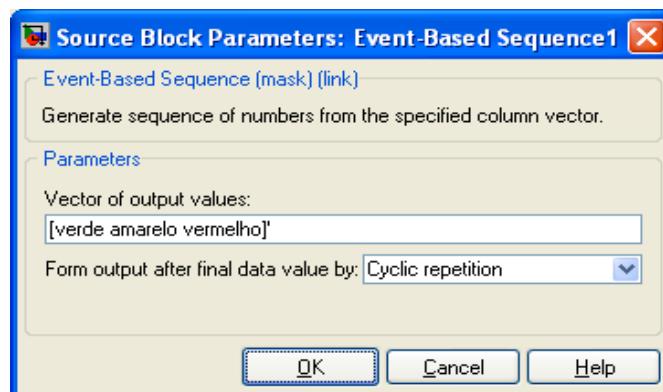


Figura 5 – Janela de propriedades do bloco Event-based Sequence.

3. Realiza a leitura do sinal gerado no bloco dois, referente à duração do estágio do semáforo, e gera com seu valor um atributo para a entidade gerada no bloco um. Como resultado, a entidade passará a transportar a duração do respectivo estágio que ao qual representa.
4. Representa uma fila do tipo *first-in-first-out* (primeiro a entrar é o primeiro a sair) necessária para uniformizar a geração do sinal. O controle de fila neste ponto faz-se necessário porque o bloco sete, que será explicado adiante, retém as entidades por determinado intervalo de tempo, travando sua porta de entrada e, por consequência, travando toda a troca de sinal dos blocos antecessores. Com a existência do bloco de fila, as entidades geradas serão armazenadas e a geração do sinal para sua geração poderá continuar a ocorrer a intervalos constantes, sem interrupção.
5. Transforma a entidade que chega ao bloco no instante de execução em uma chamada de função, cujo objetivo final é gerar o sinal discreto para o controle do semáforo, e que será descrito a seguir. Após a chamada da função, a entidade segue o fluxo a partir da porta *OUT* em destino ao bloco oito.
6. Função cujo objetivo é gerar o sinal discreto para cada estágio do semáforo. O bloco de função é um subsistema, uma vez executado, gera um sinal sequencial definido nas propriedades do bloco através de um vetor unidimensional.
7. Fornece uma porta de saída para o sinal discreto de controle do semáforo gerado, para ser consumido externamente.
8. Responsável por controlar a duração do sinal (estágio). Atua como um servidor de entidades que serve cada entidade, individualmente, durante certo intervalo de tempo. A duração do serviço é definida através do atributo que cada entidade carrega (duração do estágio). Dessa forma, tem-se a geração de cada sinal do estágio do semáforo a intervalos de tempo individuais, pois cada entidade gerada (estágio) é convertida num sinal discreto através do bloco seis e este sinal é externado do subsistema através da porta sete, sendo a duração do sinal controlada pelo servidor que, enquanto serve uma entidade, não permite que outra seja processada. Portanto, enquanto uma entidade é servida, o subsistema trava e nenhum outro sinal é gerado, permanecendo o sinal gerado anteriormente inalterado.
9. Fornece um mecanismo para encerrar o caminho de uma entidade ao longo do modelo. Entidades que atingem este bloco cumpriram seu objetivo e são descartadas do sistema.

6. Simulação

A Figura 6 mostra um sinal gerado pelo subsistema num intervalo de dois minutos, considerando os tempos de cada estágio, definidos para o modelo.

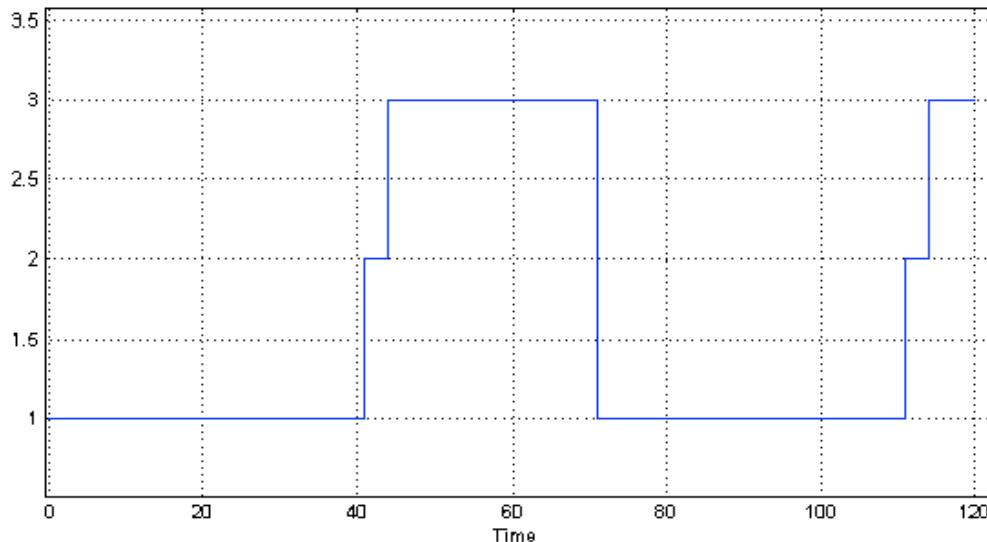


Figura 6 - Exemplo de sinal para controle dos estágios do semáforo

O período de simulação foi de quatro horas. A escolha do período foi arbitrária. O volume dos resultados colhidos não permite uma demonstração adequada para realização de análises; no entanto, o objetivo era avaliar a estabilidade do modelo durante a simulação. A Figura 7 mostra os sinais para simulação da demanda de veículos nas aproximações:

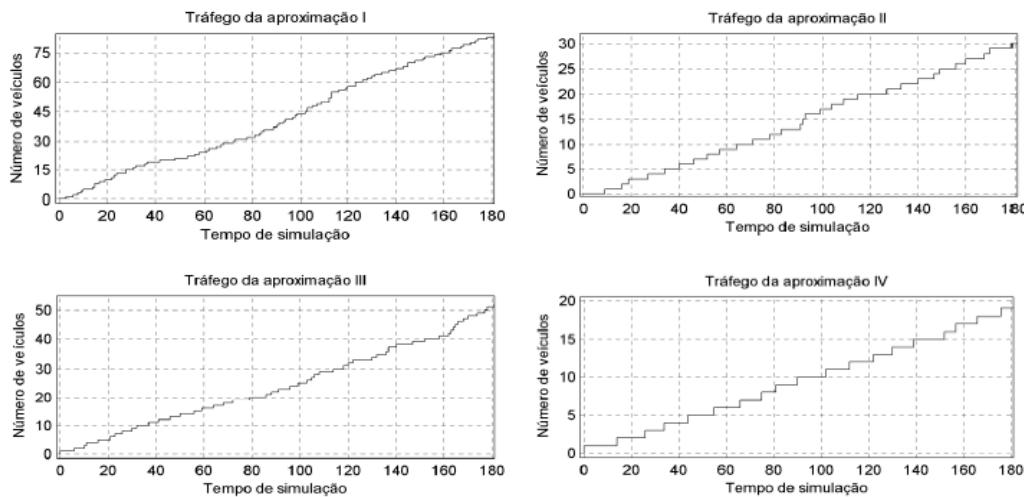


Figura 7 – Sinais para simulação da demanda de veículos nas aproximações

A Figura 8 apresenta sinais colhidos na simulação da demanda de veículos:

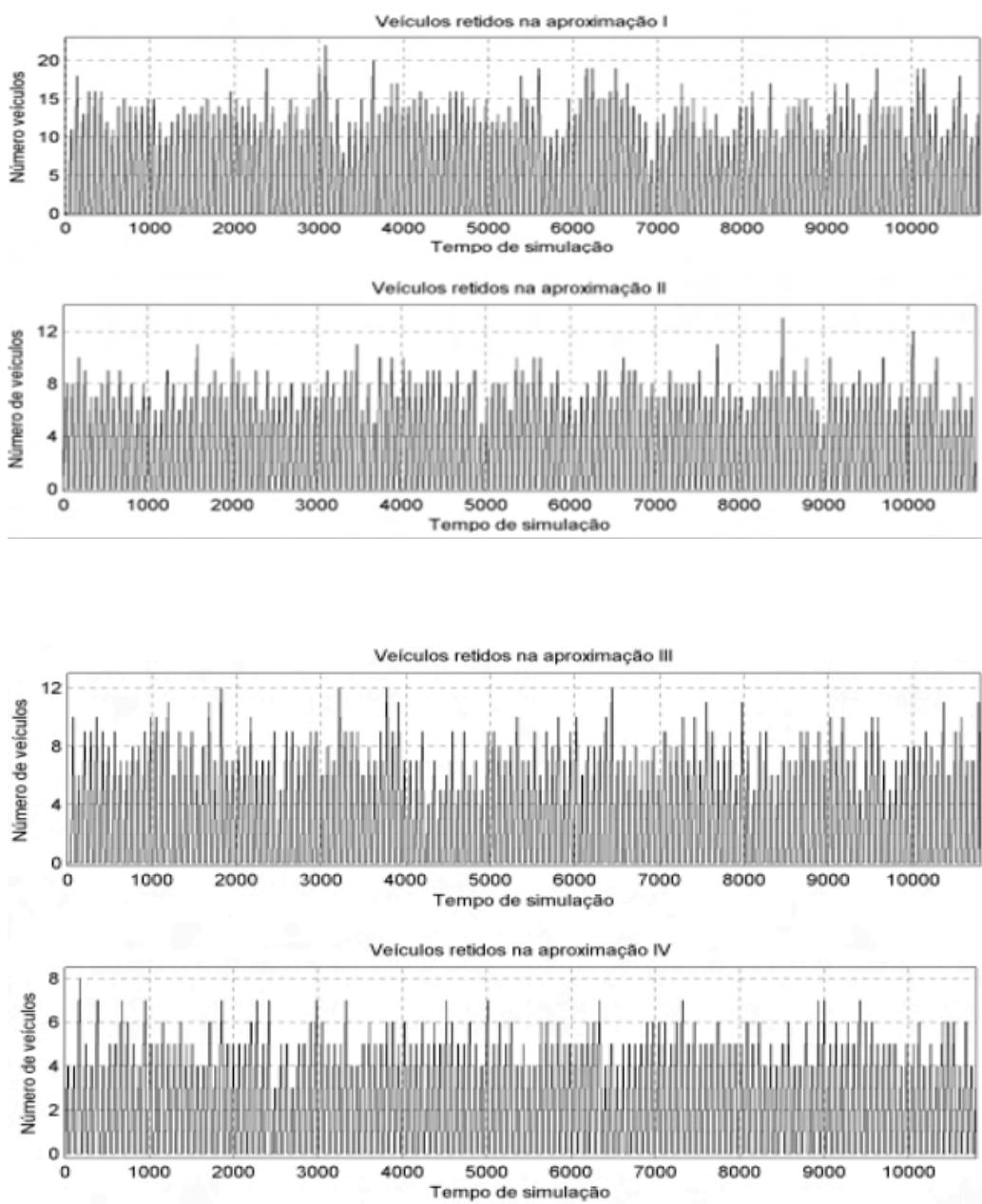


Figura 8 – Sinais para simulação da demanda de veículos colhidos na simulação.

Através do gráfico é possível concluir que o mecanismo de retenção de veículos do controle semafórico se manteve estável ao longo de toda a simulação. Nos gráficos obtidos no tempo de travessia nas aproximações colhidos na simulação, também não foram observadas distorções. A inexistência de picos e deformações permitem concluir que o sistema apresentou um padrão consistente de operação. E por fim, a estabilidade

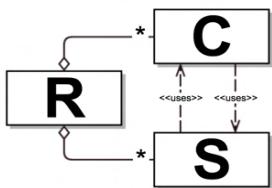
do sistema foi possível de ser evidenciada com o último teste realizado com a vazão dos semáforos colhidos na simulação.

7. Considerações Finais

O trabalho apresentou resultados bastante satisfatórios na utilização de técnicas de modelagem e simulação computacional para estudos de sistemas dinâmicos. A ferramenta Matlab/Simulink também contribuiu para o desenvolvimento e execução do trabalho. Acredita-se que o modelo gerado e testado neste trabalho possa ser utilizado como base para o desenvolvimento de modelos mais abrangentes que visam o estudo do tráfego urbano de veículos.

Referências Bibliográficas

- Denatran. (1984). *Manual de Semáforos*, 2º edição. Brasília.
- Freitas Filho, P. J. (2008). *Introdução à Modelagem e Simulação de Sistemas – Com Aplicações em Arena*. Florianópolis. Editora Visual Books.
- Gucci, J. Neto. (1996) *Aplicações da engenharia de tráfego na segurança dos pedestres*. São Paulo. 1996. Dissertação (Mestrado em Engenharia) – Universidade de São Paulo, São Paulo.
- Ipea. (1997). *Redução das Deseconomias Urbanas pela Melhoria do Transporte Público*. [s.l.] 1997. Disponível em: http://www.ipea.gov.br/pub/livros/l_avul.html. Acesso em: 10 nov. 2009.
- Matsumoto, E. Y. (2003). *Simulink 5: fundamentos*. São Paulo. Editora Érica.
- Portugal, L. da S. (2005). *Simulação de Tráfego – Conceitos e Técnicas de Modelagem*. Rio de Janeiro. Editora Interciênciacia.



Service Oriented Architecture (SOA) Integration with Industrial Machinery

Leonardo Rafaeli, Laercio Cruvinel

Faculdade de Computação e Informática (FCI) – Universidade Presbiteriana Mackenzie
Higienópolis – São Paulo – SP – Brazil

leonardo.rafaeli@gmail.com, laercio.cruvinel@mackenzie

Abstract. This article describes the usage of Service-Oriented Architecture in the industrial segment, showing the motivations and advantages of the approach, but also the challenges and implementation issues for this architecture model.

Resumo. Esse artigo mostra a utilização da Arquitetura Orientada a Serviços no segmento industrial, mostrando suas motivações e vantagens, além dos desafios e dos problemas que podem ser encontrados ao implantar esse modelo de arquitetura.

1. Introduction

Corporate systems are evolving fast, thanks to increased processing power and to the need of overcome competitors, demanding big investments but making systems more mature and efficient for the execution of business processes.

The usage of Service-Oriented Architecture (SOA) has allowed enterprise IT to grow in an ordered fashion, reusing business components already developed and, mainly, easing the integrations of different systems in the corporate context.

As a result, business processes can now be soft-integrated with machinery, either manufacturing or for industrial automation, with great abstraction from programming and from complex interactions among the target systems.

In this article, we will discuss some motivations, advantages and challenges of such integration, presenting a case study based on a prototype work where implementation issues are also shown. Section I is this Introduction. In Section II we review some concepts of SOA and of Complex Event Processing (CEP), while Section III presents the means of integrating industrial machinery with higher levels of software architecture. Finally, in Section IV we draw some conclusions and suggestions for future work.

2. SOA and CEP

Whenever integrations involve physical devices, namely in the case of industrial automation, systems exposing the machines' functionalities are in need of a manual

initial programming – the code to be executed by the devices needs to be developed and implemented by a human programmer. Additionally, adapters need to be developed in order to allow talking to the low level languages of the machinery controllers. A possible consequence is the lack of professionals with adequate knowledge of such languages.

It is noticed that there is a significant initiative for industrial equipment when it comes to adoption of standardized technologies in enterprise systems architecture. The fierce competition that companies are facing in the current market has resulted in increased investment in research and development, and improvements such as in the purchase of modern equipment.

The integration of these devices also require significant costs for companies, making them lose time-to-market deployment of their software or industrial automation tools, and that "currently, one third of the costs in a manufacturing business is spent on installation and configuration of equipment " (JAMMES and SMIT, 2006).

With the increased processing power of controlling this machinery, programming these devices is becoming easier using languages of higher levels. Nowadays, there already exist devices that operate through network protocols such as SNMP, exposing certain features, which can be invoked over the network by customers using this protocol.

However, no big processing and memory requirements are in need when managing the industrial machinery. Also well-known is the fact that the development of Web Services, although not inherently complex, requires high processing capabilities of servers, primarily driven by converting and transforming XML content into data that is ready to be processed.

In matters of software and systems architecture, one of the next steps in a service-oriented architecture is the adoption and management of Complex Event Processing (CEP), which is a basic component of analysis of real-time business intelligence (LUCKHAM and SCHULTE, 2012). With the adoption of CEP, it is possible to add intelligence to information that travels on the service bus, in an organized, quick and easy to understand way. For example, consider a Telecom business environment where there is a drop in requests for new services. One can set an event such that, when a critical level is reached, a notification is automatically sent to those responsible for products or corporate strategy so an action plan can be developed, such as promotions and so forth. Exposing these services may imply creating a governance of the features available within the corporation, reusing rules and automating calls even when complex business rules are involved.

As SOA adoption in business is increasing, there is a need to bring large IT processes closer to the business area, making the whole IT aligned with these high-level business processes and with systems outside from the user's view, such as mainframe systems and Big Data. CEP allows abstracting from the layers where there is a great demand for low-level technical services, at the same time managing to add the SOA value to the IT assets, listening to the data on the service bus and invoking processes according to defined rules.

Currently, there are tools that implement the concepts of CEP usually deployed in the Enterprise Service Bus (ESB), such as EPO (Oracle Event Processing), which belongs to the Oracle SOA Suite.

3. Integration with Industrial Machinery

With the various architectural models available, it is possible to enable communication between industrial machinery and corporate systems that operate in any segment of business, at the same time receiving the benefits that SOA brings.

One way of enabling this communication between the services available in a service-oriented architecture and the controllers of the machines is "using a *Cell Controller* that performs command and control functions usually installed on a PC" (KOMODA, 2006). With it, it is possible to receive data from machines on the PC and send it to the service bus, as shown in Figure 1.

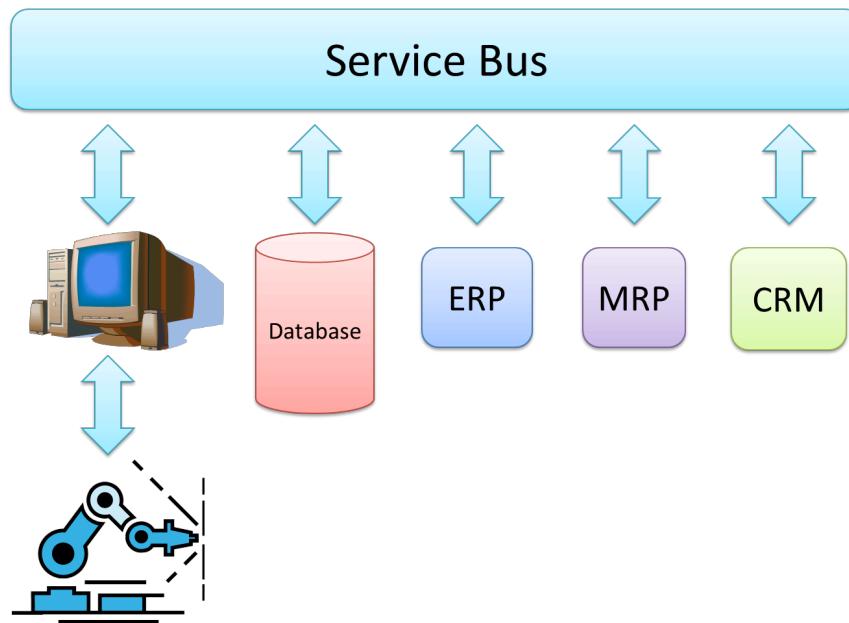


Figure 1: Integration among machines and enterprise systems.

One of the biggest challenges to promote real-time communication of enterprise systems with industrial machinery is the latency. Due to this, Internet communications are not advisable, and local network connections should be used to ensure the on-time delivery of data sent by the machines, such as sensors, motors, or even sending tasks through other systems, like a MRP, CRM or a Web application.

4. Conclusion

The ability to abstract behaviors and details of communication between industrial systems and enterprise systems helps the understanding of developed services and the applied business rules, resulting in greater productivity and reduced costs for companies which need to evolve the business.

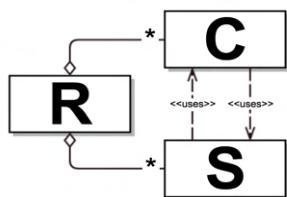
This evolution involves technical issues about the processes themselves, such as adding new modules to interpret the communication of the machines with the services, implementing fault tolerance both in industrial machinery and in the service bus, and increasing control over IT assets that were developed, creating new business functions and applying governance processes.

The visibility of business rules facilitates the understanding of the processes and also allows the creation of scenarios in order to simulate problems, enabling industries to test their mechanisms of risk management where extreme situations can impact the production or service delivery.

Finally, it is clear that there is great advantage in the adoption of service-oriented architecture by companies as the benefits make them more prepared for an upcoming scenario where changes are becoming more frequent and competition is becoming fiercer. With an adequate architecture defined and implemented, forecasts are more precise when changes are made, and so are simulations of operating and evolving costs. The same is true for the analysis of alternative scenarios, ensuring the best decisions are taken in the process of improvement.

References

- Erl, T. (2005) “Service-Oriented Architecture - Concepts, Technology, and Design”. Toronto/ON, Canada: SOCS.
- Jammes, F. and Smit, H. (2006) “Service-Oriented Paradigms in Industrial Automation”, In: IEEE Trans. Industrial Informatics 1(1):62-70.
- Komoda, N. (2006) “Service oriented architecture (SOA) in industrial systems”, In: IEEE International Conference on Industrial Informatics, pp. 1-5.
- Luckham, D. and Schulte, W.R. (2012) “Complex Event Processing and the Future of Business Decisions”, In: Complex Event Processing & Real Time Intelligence, available online: <http://www.complexevents.com/2012/07/12/>. Accessed in: May 27, 2013.



Arquitetura Corporativa: Conceituação e Comparaçāo dos Frameworks ZACKMAN e TOGAF

Douglas C. Santos, Fábio S. Lopes, Takato Kurihara

Faculdade de Computação e Informática, Universidade Presbiteriana Mackenzie
 douglas.carleal@mackenzie.com.br, flopes@mackenzie.br,
 takato@mackenzie.br

Abstract. *In the last few years, Corporate Architecture has gain space in the academic and corporate sectors. The process is directly linked to the IT infrastructure and the organization of the business process seeking a pattern of operational models of the companies. Several frameworks have been presented with methods, schemes and examples with the purpose of assisting in the creation of a better solution for each company. This work focused the study and comparison of the two most popular models TOGAF and ZACKMAN concluding that both practices are complementary.*

Resumo. *Nos últimos anos, o assunto Arquitetura Corporativa vem ganhando espaço nos meios acadêmicos e empresariais. O processo está diretamente relacionado com a infraestrutura de TI e a organização dos processos de negócios, visando uma padronização de modelos operacionais das empresas. Vários frameworks foram propostos oferecendo metodologias, esquemas e exemplos com o intuito de auxiliar na construção de melhor solução para cada empresa. Este trabalho teve como foco o estudo e comparação de dois modelos mais populares TOGAF e ZACKMAN, concluindo que as duas práticas são complementares.*

1. Introdução

A Tecnologia de Informação (TI), na maioria das empresas, já faz parte do modelo de negócio de suas empresas. No mercado, existem diversas metodologias e frameworks que propiciam às corporações obterem meios de mensurarem e administrarem seus ativos de TI, além de formas de alinharem e direcionarem seus investimentos nesta área, que estejam plenamente compatíveis com as áreas de negócio. Entre varias metodologias, está a Arquitetura Corporativa que tem a função de proporcionar uma visão de longo prazo dos processos, sistemas e tecnologias das empresas [ROSS; WEILL; ROBERTON, 2008].

O objetivo do artigo é apresentar os conceitos de Arquitetura Corporativa que vem sendo considerados relevantes nas organizações, e explorar dois modelos populares de *frameworks* disponíveis no mercado fazendo uma comparação entre eles.

Quanto a metodologia, é uma pesquisa descritiva, segundo Gil [2010] onde, reuniu-se um conjunto de documentos que detalham os modelos de Arquitetura Corporativa escolhidos para formar um arcabouço literário como fonte de dados. Este material foi organizado e estruturado para análise comparativa.

2. Frameworks de Arquitetura Corporativa

De acordo com Cambiucci [2010], “um *framework* de arquitetura oferece um conjunto bem definido de fases, atividades, documentos, processos, *templates*, recomendações e métricas para a execução de uma arquitetura corporativa”. Há outras definições como do próprio autor da ferramenta, Zackman e do grupo TOGAF.

3. Zachman Framework

O Zachman *framework* leva o nome de seu criador John A. Zachman. É um dos mais conhecidos *frameworks* de Arquitetura Corporativa existentes no mercado e um dos precursores também; seu artigo “A framework for information systems architecture” publicado em 1987 é considerado um dos primeiros registros da Arquitetura Corporativa [ZACKMAN, 1987]. Na mais recente publicação, Zachman mudou o conceito inicial de seu *framework*, proposto apenas para Sistemas de Informações (TI) como estava no título de seu artigo de 1987, e passou a descrever aplicando à empresa como um todo. “Arquitetura é uma questão corporativa, e não uma questão de Sistema”. E justifica dizendo: “Hoje eu diria que o objeto final para o engenheiro e fabricante é a Empresa, não apenas desenvolver e implantar sistemas” [ZACKMAN, 2007].

O detalhamento das perspectivas e abstrações do Sowa [1992] mostrado na Figura 1, apresentado na forma de uma matriz, permite um melhor entendimento do Zachman *Framework*.

Perspectivas	Abstrações					
	O que Dados	Como Processos	Onde Localização	Quem Responsabilidades	Quando Tempo	Porque Motivação
Planejadores Escopo						
Proprietários Negócio						
Desenvolvedores Sistema						
Construtores Tecnologia						
Implementadores Configuração						
Usuários Implementação						

Figura 1 – Perspectivas e Abstrações.

4. The Open Group Architecture Framework (TOGAF)

Segundo The Open Group [2011] este *framework* teve sua primeira versão lançada em 1995 e foi baseado no *Technical Architecture Framework for Information Management* (TAFIM) , que foi desenvolvido pelo Departamento de defesa dos Estados Unidos.

Segundo Zackman [2007], o TOGAF definido por The Open Group provê os métodos e ferramentas para auxiliar a produção, o uso e manutenção de uma arquitetura corporativa. É baseado em um processo interativo apoiado por boas práticas e um conjunto reutilizável de ativos arquitetônicos.

Ainda, de acordo com The Open Group [2011], com relação a sua estrutura, a versão mais atual do TOGAF está dividido em sete partes e apresenta itens como: Metodologia de Desenvolvimento da Arquitetura, Diretrizes e Técnicas do Adm, Framework de Arquitetura de Conteúdo, Framework de Competência da Arquitetura.

5. Análise comparativa entre TOGAF e ZACHMAN framework

Apesar de TOGAF e Zachman se autodenominarem como *Frameworks*, alguns especialistas em Arquitetura Corporativa não dizem o mesmo, por exemplo, Sessions [2007] diz que Zachman *Framework* seria na verdade definida como uma taxonomia em função de ter um foco expressivo na classificação dos artefatos. Enquanto o TOGAF é melhor definido como um processo, especialmente por causa da *Model Driven Architecture* - MDA .

Outro fator importante a observar entre ambos os modelos que complementa, é que Zachman privilegia a classificação e os papéis dos envolvidos, ou seja, o Planejador, Proprietário, Desenvolvedor, Construtor e o Usuário, portanto abrange todos os aspectos relacionados à responsabilidades da organização. Enquanto o TOGAF por sua vez proporciona uma elaboração da arquitetura desde o seu início, por causa das fases da MDA (A, B, C, D, E, F, G) graças à sua orientação por processo possibilita ter um controle, um passo a passo, durante a execução da arquitetura.

A Figura 2 apresenta as vantagens e desvantagens baseada no estudo.

	TOGAF	ZACHMAN
Pontos Fortes	<ul style="list-style-type: none">· Foco na metodologia· Documentação disponível gratuitamente na internet	<ul style="list-style-type: none">· Foco na organização e Classificação dos artefatos· Delimitação dos papéis dos envolvidos no processo.
Pontos Fracos	<ul style="list-style-type: none">· Não garante a entrega de uma boa arquitetura· Permite “pular” alguns passos do MDA	<ul style="list-style-type: none">· Não possui metodologia· A documentação é restrita· Não garante que a arquitetura entregue será a melhor que atual

Figura 2 – Pontos Fortes e Pontos Fracos .

O que há em comum entre Zachman *Framework* e TOGAF? Após análise e comparação, além de vantagens e desvantagens, observa-se que o ponto comum entre esses

frameworks está na razão de sua existência, que é o alinhamento das áreas de negócios com TI. Suas abordagens são distintas, não sendo possível encontrar pontos de convergência. No entanto, Zachman e TOGAF se complementam de modo a potencializar a implantação de uma Arquitetura Corporativa.

6. Considerações finais

Esse trabalho abordou conceitos de Arquitetura Corporativa, e explorou dois *frameworks* conhecidos do mercado, preparando um quadro comparativo sobre os pontos existentes nos dois *frameworks*.

Como resultado concluiu-se que os modelos estudados divergem nas suas abordagens. O *framework* Zachman apresenta uma matriz visual de artefatos arquitetônicos, enquanto o TOGAF oferece uma metodologia. Eles podem ser implantados de forma complementar, ou seja, a Arquitetura Corporativa não precisa ser necessariamente composta por apenas um *framework*. Além de não existir um modelo que domine esse ecossistema, reforça-se que o TOGAF, na maioria dos casos, é utilizado como ponto de partida para a elaboração da Arquitetura Corporativa, mesmo que inicialmente não garanta a entrega de uma “boa” Arquitetura. Fica como contribuição, uma sugestão para ampliar o estudo para outros *frameworks* existentes no mercado.

Referências Bibliográficas

- Cambiucci, W. (2010) Biblioteca MSDN. Enterprise Architecture: A arquitetura corporativa e o papel do arquiteto de TI, 2010. Disponível em: <<http://msdn.microsoft.com/pt-br/library/gg490650.aspx>>. Acesso em: 18 Novembro 2011.
- Gil, A. C. (2010) Como elaborar projetos de pesquisa. 3 ed. ed. São Paulo: Atlas.
- Ross, J. W.; Weill, P.; Robertson, D. C. (2008). Arquitetura de TI como Estratégia Empresarial. São Paulo: M. Books do Brasil Editora Ltda.
- Sessions, R. (2007). Uma comparação entre as quatro principais metodologias de arquitetura corporativa. Biblioteca MSDN. Disponível em: <<http://msdn.microsoft.com/pt-br/library/bb466232.aspx>>. Acesso em: 06 Março 2012.
- Sowa, J. F.; Zachman, J. A. (1992). Extending and formalizing the *framework* for information systems architecture. IBM Systems Journal, v. 31, n. 3.
- The Open Group. (2011). TOGAF Version 9.1. Open Group Standard. Disponível em: <<http://pubs.opengroup.org/architecture/togaf9-doc/arch/>>. Acesso em: 18 abr. 2012.
- Zackman, J. A.(1987). A *framework* for information systems architecture. IBM Systems Journal, v. 26, n. 03, p. 276-292.
- Zackman, J. A.(2007). Architecture Is Architecture Is Architecture. [S.l.].

A Direct Proof of the Continuity of Non-Degenerate Minimum Stable Distributions

Wagner de Souza Borges¹, João Maurício Araújo Mota²

¹Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Rua da Consolação 930 – 01.302-907 – São Paulo – SP – Brazil

²Departamento de Estatística e Matemática Aplicada – Universidade Federal do Ceará (UFC)
Fortaleza – CE – Brazil.

wborges@mackenzie.br, oiciruam@ufc.br

Abstract. It is a well known result in extreme value theory that if for a sequence $\{\xi_n : n \geq 1\}$ of independent and identically distributed random variables one can find real constants $\alpha_n > 0$ and β_n , $n \geq 1$, such that $\{(\min\{\xi_1, \dots, \xi_n\} - \beta_n)/\alpha_n : n \geq 1\}$ has a non-degenerate limiting distribution G , then there are only three possible continuous limiting types for G . The result, due to [Fisher and Tippett 1928] and [Gnedenko 1943], relies on the analysis of certain functional equations whose solutions are necessarily continuous. This fact raises the natural question of whether the continuity and maybe other properties of minimum stable distributions follow directly from its definition. In this article a direct proof of their necessary continuity is presented.

Resumo. Um resultado conhecido da teoria de valores extremos é que se para uma sequência $\{\xi_n : n \geq 1\}$ de variáveis aleatórias independentes e identicamente distribuídas é possível encontrar constantes reais $\alpha_n > 0$ and β_n , $n \geq 1$, tais que $\{(\min\{\xi_1, \dots, \xi_n\} - \beta_n)/\alpha_n : n \geq 1\}$ tem uma distribuição limite não-degenerada G , então existem apenas três tipos contínuos possíveis para a distribuição limite G . Este resultado, que se deve a [Fisher and Tippett 1928] and [Gnedenko 1943], decorre da análise de certas equações funcionais cujas soluções são necessariamente contínuas. Este fato suscita, naturalmente, a seguinte questão: seria possível demonstrar a continuidade e talvez outras propriedades das distribuições mínimo estáveis diretamente da definição? Neste artigo, apresenta-se uma demonstração direta da necessária continuidade dessas distribuições.

1. Introduction

Extreme value theory deals, among other things, with the derivation of approximate distributions for the maximum and the minimum values observed in simple random samples. The formal setting is that in which

$$M_n = \min\{\xi_1, \dots, \xi_n\}, \quad n \geq 1,$$

where ξ_1, ξ_2, \dots are independent and identically distributed random variables defined on the same probability space, (Ω, \mathcal{F}, P) , and one is interested in:

1. whether there are real constants, $\alpha_n > 0$ and $\beta_n, n \geq 1$, and a distribution function, G , such that

$$\lim_{n \rightarrow \infty} P\left\{ \frac{M_n - \beta_n}{\alpha_n} \leq x \right\} = G(x),$$

for all x in the continuity set of G ; and, if this is the case,

2. what properties does G have.

In this context we say that G a limiting distribution for $\{M_n\}_{n=1}^{\infty}$ and it is well known that if G is nondegenerate, then it must be one of the following types:

- (a) $G_1(x) = 1 - e^{-x^\lambda}$, for $x \geq 0$, where $\lambda > 0$;
- (b) $G_2(x) = 1 - e^{-(x)^{-\lambda}}$, for $x \leq 0$, where $\lambda > 0$; or
- (c) $G_3(x) = 1 - e^{-e^x}$, for $-\infty < x < +\infty$.

A demonstration of the above result, due to [Fisher and Tippett 1928] and [Gnedenko 1943], can be found in [Barlow and Proschan 1975] and it relies on the solution of the following three functional equations:

- (d) $\bar{G}^n(\alpha_n x) = \bar{G}(x)$, with $G(x) = 1 - \bar{G}(x) = 0$ for $x \leq 0$;
- (e) $\bar{G}^n(\alpha_n x) = \bar{G}(x)$, with $G(x) = 1 - \bar{G}(x) = 1$ for $x \geq 0$;
- (f) $\bar{G}^n(x + \beta_n) = \bar{G}(x)$, for $x \in \mathbb{R}$,

derived from the analysis of the normalizing real constants, $\alpha_n > 0$ and $\beta_n, n \geq 1$, in following definition.

Definition 1. A distribution function G is minimum stable iff there exist real constants $\alpha_n > 0$ and $\beta_n, n \geq 1$ such that

$$\bar{G}^n(\alpha_n x + \beta_n) = \bar{G}(x), \text{ for all } x \in \mathbb{R}.$$

The defining equality of minimum stability can be rephrased in terms of the concept of distribution type stated below

Definition 2. The distribution functions G and H are of the same type iff there exist real constants $\alpha > 0$ and β , such that

$$\bar{G}(\alpha x + \beta) = \bar{H}(x), \text{ for all } x \in \mathbb{R}.$$

According to definitions 1 and 2, a distribution function G is minimum stable if and only if for every $n \geq 1$, $H_n = 1 - \bar{G}^n$ and G are of the same type.

Limiting distributions and type are connected by the following result, whose proof can be found in [Feller 1966].

Lemma 1. Let G and H be nondegenerate distribution functions. If $\{F_n\}$ is a sequence of distribution functions such that:

1. there exist real constants $\alpha_n > 0$ and $\beta_n, n \geq 1$ such that

$$\bar{F}_n(\alpha_n x + \beta_n) \rightarrow \bar{G}(x) \text{ for all } x \in \mathbb{R};$$

2. there exist real constants $\gamma_n > 0$ and δ_n , $n \geq 1$ such that

$$\overline{F}_n(\gamma_n x + \delta_n) \rightarrow \overline{H}(x) \quad \text{for all } x \in \mathbb{R},$$

then G and H are of the same type.

The following result links the concept of minimum stability to the limiting distribution of the sequence $\{M_n\}_{n=1}^{\infty}$.

Theorem 1. G is a continuous limiting distribution for $\{M_n\}_{n=1}^{\infty}$ if and only if G is minimum stable.

Remarks.

1. The proof of Theorem 1 is elementary. The argument is that of [Barlow and Proschan 1975], page 232, Theorem 2.1, except that continuity of G is not assumed there. The assumption, however, must be made since the defining equality of minimum stability must hold for all $x \in \mathbb{R}$. In order to prove the if part of the theorem we need to show that minimum stable distributions are continuous, which is done in the next section. To the authors knowledge the proof provided is new.
2. For details of the afore mentioned analysis of the normalizing constants see [Barlow and Proschan 1975], pages 232-234, Lemmas 2.2 - 2.6
3. The solution of the above functional equations require the notion of regular variation, introduced by [Karamata 1930]. For details, see [Barlow and Proschan 1975], pages 234-236, Lemma 2.7, definition 2.8, Lemma 2.9 and Theorem 2.10.

2. Main Result

Theorem 2. Every non-degenerate minimum-stable distribution function, G , is continuous.

proof. For any distribution function, G , its continuity on $\{G = 0\}$ is immediate for if $x \in \mathbb{R}$ is such that $G(x) = 0$ then $G(y) = 0$ for any $y < x$, which implies that $G(x-0) = G(x)$ (Recall that G is always right continuous).

In view of the above remark, to establish the continuity of a non-degenerate minimum-stable distribution function, G , it suffices to prove that G is also left continuous on $\{G > 0\}$ or, equivalently, that \overline{G} is left continuous on $\{\overline{G} < 1\}$.

Recall from Theorem 1 that a distribution function G is minimum stable if and only if, for each $n \in \mathbb{N}$, there are real constants $\alpha_n > 0$ and β_n such that

$$\overline{G}^n(\alpha_n x + \beta_n) = \overline{G}(x) \quad \text{for all } x \in \mathbb{R}.$$

Alternatively, G is minimum stable if and only if, for each $n \in \mathbb{N}$, there are real constants $\alpha'_n > 0$ and β'_n such that

$$\overline{G}^n(x) = \overline{G}(\alpha'_n x + \beta'_n) \quad \text{for all } x \in \mathbb{R}.$$

Let us now fix $x \in \{\bar{G} < 1\}$ and assume that

$$\bar{G}(x-0) - \bar{G}(x) = \epsilon > 0.$$

If for some $y < x$

$$1 > \bar{G}(y) \geq 1 - \frac{\epsilon}{2},$$

then

$$\bar{G}^n(y) - \bar{G}^{n+1}(y) = \bar{G}^n(y)[1 - \bar{G}(y)] \leq \frac{\epsilon}{2}$$

and consequently

$$\bar{G}(x) \leq \bar{G}^k(y) = \bar{G}(\alpha'_k y + \beta'_k) \leq \bar{G}(x-0),$$

for some integer $k \in \mathbb{N}$, since $\lim_{n \rightarrow \infty} \bar{G}^n(y) = 0$. But this contradicts the fact that \bar{G} is discontinuous at x since \bar{G} cannot take values between $\bar{G}(x)$ and $\bar{G}(x-0)$.

From the above observation, in order to prove that \bar{G} is left continuous on $\{\bar{G} < 1\}$, it suffices to show that for any $x \in \{\bar{G} < 1\}$ and $\epsilon > 0$, there exists $y < x$ such that

$$1 > \bar{G}(y) \geq 1 - \frac{\epsilon}{2}.$$

For that, let

$$z = \sup\{y < x : \bar{G}(y) \geq 1 - \frac{\epsilon}{2}\}$$

and observe that

$$\bar{G}(z) = \bar{G}(z+0) \leq 1 - \frac{\epsilon}{2} < 1 \quad (1)$$

and

$$\bar{G}(z) = \bar{G}^2(\alpha_2 z + \beta_2) \geq \bar{G}^2(z) \quad (2),$$

since $\bar{G}(z) < 1$.

Consequently,

$\alpha_2 z + \beta_2 < z$ (since the fact that G non-degenerate excludes equality

and

$$1 > \bar{G}(\alpha_2 z + \beta_2) \geq 1 - \frac{\epsilon}{2},$$

for if $\bar{G}(\alpha_2 z + \beta_2) = 1$ would lead to a contradiction between (1) and (2).

QED

Referências

- Barlow, R. A. and Proschan, F. (1975). *Statistical Theory of Reliability and Life Testing*. New York: Holt, Rinehart and Winston, Inc.
- Feller, W. (1966). *An Introduction to Probability Theory and Its Applications, Vol. I*. New York: John Wiley and Sons.

- Fisher, R. A. and Tippett, L. H. C. (1928). Limiting forms of the frequency distribution of the largest or smallest member of a sample. In *Proc. Cambridge Philos. Soc. V XXIV*, pages 180–190.
- Gnedenko, B. V. (1943). Sur la distribution limite du terme maximum d'une série aléatoire. In *Ann. of Math. 44(3)*, pages 423–453.
- Karamata, J. (1930). Sur un mode de croissance régulière des fonctions. In *Mathematica (Cluj)*, pages 38–53.