

O Processador Intel Core i7

Bruno Teles

Instituto de Computação
Universidade Estadual de Campinas

Av. Albert Einstein, 1251
55-19-35215838

seletonurb@gmail.com

ABSTRACT

Neste paper, são descritas características do processador quadcore da Intel Core i7, como seu datapath, gerenciamento de memória, gerenciamento de energia e ganhos de desempenho que podem ser obtidos com as inovações.

Categorias e Descritores de Temas

C.1.2 [Processor Architectures]: Multiple Data Stream Architectures (Multiprocessors) – *Interconnection architectures, Multiple-instruction-stream, multiple-data-stream processors (MIMD)*.

Termos Gerais

Measurement, Documentation, Performance, Design.

Palavras-Chave

Microarquitetura, Nehalem, quadcore, memória cache, consumo de energia, multithread.

1. INTRODUÇÃO

No fim de 2008, a Intel lançou seu novo processador quad-core. Sob o nome de Core i7, este é o primeiro processador baseado na micro-arquitetura Nehalem. Os processadores Intel Core i7 oferecem uma série de inovações em desempenho quad-core e contam com avançadas tecnologias de processador. Esta nova micro-arquitetura não prevê uma mudança tão radical quanto a passagem de Netburst (Pentium 4) para Core2, pelo menos não em um nível tão baixo. O que não significa que não venha a trazer ganhos significativos em desempenho.

Tomando como base os núcleos Core2, a Intel se questionou sobre o que se poderia ser feito para obter processadores ainda melhores. Além de melhorias na já excelente micro-arquitetura, uma das principais mudanças, ou pelo menos a que chama mais atenção é que finalmente a controladora de memória foi integrada ao processador, aposentando o esquema de FSB e Northbridge,

aproveitando a oportunidade para a implementação de um novo barramento; serial, ponto-a-ponto, bi-direcional e de baixa latência: o QPI (Quick Path Interconnect); para conexão do processador com o chipset ou outros processadores. Adicionado a isto, será feita menção à retomada do HyperThreading, à utilização do Turbo Boost e à organização da memória, cruciais para a compreensão do funcionamento desta arquitetura.

2. A ARQUITETURA NEHALEM

2.1 Visão Geral

A micro arquitetura Nehalem substitui a arquitetura Core2 em praticamente todas as frentes: desde processadores para dispositivos móveis de baixíssimo consumo até potentes servidores, passando principalmente pelo desktop. Esta micro arquitetura toma como base o excelente núcleo da micro arquitetura Core2, inovando fundamentalmente nos componentes ao redor do núcleo, com destaque para a controladora de memória e a interconexão por QPI.

Apesar de obsoleto para os padrões atuais, o AGTL+ (sigla de Assisted Gunning Transceiver Logic, o FSB utilizado pela Intel) é muito versátil. Sem ele não seria possível criar tão facilmente processadores dual-core e quad-core como os Pentium D e os Core 2 Quad. Sua origem está ancorada em uma característica do GTL que permite o compartilhamento do FSB por mais de um processador, até quatro processadores podem ser instalados sobre o mesmo FSB. Sobre cada FSB podem ser instalados até quatro processadores (chips), não importando quantos núcleos cada processador tenha.

Com dois processadores, o gargalo não é tão evidente. Dessa Maneira, pode-se instalar dois chips dentro do mesmo encapsulado, dobrando o número de núcleos sem grandes dificuldades técnicas (com exceção de consumo e aquecimento, que também são dobrados). O principal benefício disso é otimizar a produção. Assim, em vez de ter linhas separadas para processadores dual-core e quad-core, por exemplo, fabrica-se apenas um tipo de chip dual-core que podem dar origem tanto a processadores dual-core como quad-core. Se um Core 2 Quad fosse feito a partir de um único chip com os quatro núcleos, sua produção seria muito menor e seu preço muito maior.

Essa estratégia funciona muito bem em desktops e workstations com apenas um processador e razoavelmente bem em máquinas com dois processadores, embora exigindo o uso de um potente (literalmente, devido ao alto consumo elétrico) chipset com dois FSBs e controladora de memória de quatro canais. Já que além de potentes, os núcleos Core2 contam com enormes caches L2, equipados com agressivos sistemas de prefetch para atenuar a latência no acesso à memória.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Conference '04, Month 1–2, 2004, City, State, Country.
Copyright 2004 ACM 1-58113-000-0/00/0004...\$5.00.

Como contam com controladora de memória integrada e interconexão por QPI (barramento serial, ponto a ponto, bi-direcional e de baixa latência), os processadores Nehalem não terão empecilhos com a limitação do acesso ao chipset (onde fica a controladora de memória).

Desenvolvida com foco na modularidade, a micro arquitetura Nehalem permite que sejam criados diversos tipos de processadores, com características mais adequadas a cada segmento. Entre a biblioteca de componentes pode-se escolher de dois a oito núcleos, quantos links QPI forem necessários e até um processador gráfico.

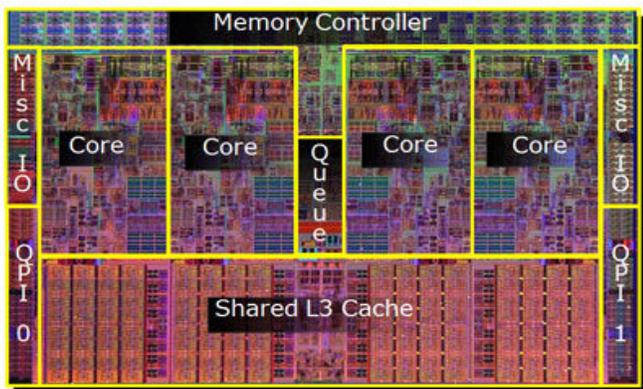


Figura 1. Foto do die do processador Nehalem.

Um ponto que merece destaque é a volta do Hyper-Threading (discutida mais detalhadamente na próxima seção), que em uma micro arquitetura de pipeline curto será muito mais útil que no Pentium4, contando ainda com o benefício da maior facilidade em trazer dados até o núcleo, tanto em função dos caches maiores, mais decodificadores e menor latência no acesso à memória graças à controladora de memória integrada. Como a tendência é o aumento da paralelização dos programas, a capacidade de executar mais threads ao mesmo tempo pode trazer ótimos ganhos em desempenho. O restante são alguns artifícios implementados para ganhar desempenho, como os feitos na revisão do Core2 de 65nm para 45nm:

- Aumento dos buffers de instruções para acomodar o maior número de instruções devido à implementação do Hyper-Threading, a reconstrução de instruções divididas entre linhas de cache foi acelerada, as primitivas de sincronização de processos foram aceleradas (importante já que cada núcleo pode trabalhar com dois threads simultaneamente).

- O predictor de desvios agora conta com dois estágios. O segundo estágio possui um histórico maior, portanto é mais lento, mas pode realizar previsões mais precisas. Normalmente a previsão do primeiro nível já é consistente o suficiente para adivinhar que caminho seguir e com a adição do segundo nível se a previsão do primeiro nível não for confiável, passa-se ao segundo. Assim diminuem ainda mais as chances de uma previsão incorreta e da necessidade de retornar até o desvio para continuar a execução, desperdiçando vários ciclos e ainda impondo uma penalização de outros tantos ciclos para reorganizar o pipeline. O que, por coincidência, também foi acelerado com a ajuda do "Renamed Return Stack Buffer", que guarda cópias dos dados já calculados.

Dessa maneira, em caso de previsão incorreta, menos dados deverão ser recalculados.

- Mais algumas instruções foram incluídas ao conjunto SSE4, com foco em processamento de texto útil para servidores de bancos de dados.

- E por fim, a TLB (Table Look-a-side Buffer, tabela para consulta rápida de endereços de memória) agora possui um segundo nível, com 512 entradas.

2.2 A Organização da Memória no Nehalem

Devido à integração da controladora de memória e ao aumento do número de núcleos dentro do chip, o arranjo de memórias cache foi refeito. O cache L1, com 32KB para dados e 32KB para instruções, foi mantido inalterado, mas o cache L2 mudou radicalmente. Com apenas dois núcleos faz sentido ter um grande cache L2 compartilhado, pois a concorrência no acesso é baixa. Mas com 4 núcleos (ou mais) a concorrência seria muito maior, prejudicando o desempenho. Por isso, foi incluído um cache L2 para cada núcleo (pequeno, mas de baixa latência), enquanto o grande cache compartilhado por todos os núcleos passa a ser o L3. Nos primeiros processadores, destinados a máquinas desktop, workstations e servidores com um ou dois processadores, o cache L3 terá respeitáveis 8MB. O cache L2 (256KB), que deve permanecer constante para todas as versões, mas o tamanho do cache L3 deve variar conforme o perfil do processador produzido, podendo também ser eliminado em processadores de baixo custo. Outro detalhe interessante na primeira geração da Nehalem é que a controladora de memória conta com três canais. A Intel anuncia que o ganho em largura de banda de memória de uma máquina Dual Nehalem sobre um Dual Harpertown ("Core2 Xeon" de 45nm com FSB1600) atual será superior a quatro vezes. E é bom ver que a Intel abandonou as memórias FB-DIMM em favor das DDR3, que consomem menos e têm latência menor. Nas plataformas Intel atuais, as memórias (FB-DIMM) e o northbridge (com dois ou quatro FSBs e controladora de memória de 4 canais) representam uma parcela considerável do consumo elétrico da máquina. Com a integração da controladora de memória no processador, o chipset deixará de consumir tanta energia, passando a um simples controlador PCI Express. Enquanto que as memórias deixarão de consumir cerca de 12W por módulo, passando para apenas 5W.

2.3 Consumo de Energia

Nesta breve análise do consumo de energia, considera-se uma máquina com dois processadores quad-core e oito módulos de memória FB-DIMM para comparação. Cada processador consome até 120 W e cada módulo de memória 12 W. Somados aos quase 40 W do northbridge, tem-se aproximadamente 375 W, sem considerar o restante da máquina. Em uma máquina semelhante, baseada em processadores Nehalem, o consumo dos processadores deve permanecer o mesmo, mas o consumo do northbridge cai para níveis desprezíveis (10 a 15 W) e mesmo aumentando o número de módulos de memória para 12 (totalizando apenas 60 W, contra 96 W dos oito módulos FB-DIMM do caso anterior) o consumo do "conjunto-matriz" deve cair para cerca de 315 W. Neste caso já pode-se constatar uma redução de pelo menos 50w no consumo, que vem acompanhado de um sensível aumento no desempenho.

3. HYPER-THREADING

A tecnologia Hyper-Threading, desenvolvida pela própria Intel, é mais uma técnica criada para oferecer maior eficiência na utilização dos recursos de execução do processador. Esta tecnologia simula em um único processador físico dois processadores lógicos. Cada processador lógico recebe seu próprio controlador de interrupção programável (APIC) e conjunto de registradores. Os outros recursos do processador físico, tais como, cache de memória, unidade de execução, unidade lógica e aritmética, unidade de ponto flutuante e barramentos, são compartilhados entre os processadores lógicos. Em termos de software, significa que o sistema operacional pode enviar tarefas para os processadores lógicos como se estivesse enviando para processadores físicos em um sistema de multiprocessamento.

A nova micro-arquitetura marca o retorno do Hyper-Threading, que cria dois núcleos virtuais a partir de cada núcleo físico. Como os Core i7 são processadores quad-core, tem-se um total de 8 núcleos virtuais. O Hyper-Threading ou SMT (simultaneous multi-threading) tem muito a oferecer em processadores mais novos como o Core i7. Por se tratarem de núcleos 4-issue wide (isto é, a cada ciclo cada núcleo faz o fetch de 4 instruções para processar), o HT tem mais oportunidades de promover um melhor aproveitamento de suas unidades de execução. Ainda mais porque há uma cache maior e uma largura de banda de memória bem mais alta. Isto é ilustrado na imagem abaixo.

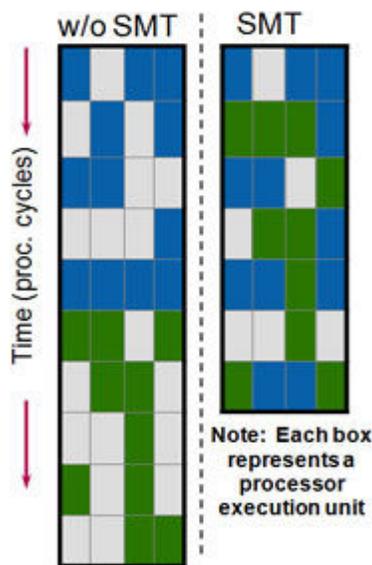


Figura 2. Cada uma das quatro unidades de execução em cada núcleo, sem o uso de HT e com o uso de HT.

Cada espaço representa uma unidade de execução. Em vez de esperar que um bloco de instruções seja executado, para então passar ao seguinte, o núcleo físico pode receber mais instruções simultaneamente com dois núcleos virtuais. Se estas forem de tipos diferentes, sua execução pode ser agendada ao mesmo tempo em que outras instruções são executadas, em outras unidades; proporcionando um significativo ganho em desempenho.

Alguns testes de desempenho feitos pela Intel mostraram que esta abordagem pode apresentar ganhos em performance em algumas aplicações específicas no Core i7. Testes mostraram que o ganho sobre operações com inteiros e com pontos flutuantes apresentaram ganhos de 13% e 7%, respectivamente. O 3DMark Vantage CPU, um simulador de física e IA apresentou um ganho de 34% quando comparado à simulação sem HT.

4. TECNOLOGIA TURBO BOOST

A tecnologia Turbo Boost, também desenvolvida pela Intel, concerne ao controle de energia e frequência de operação de acordo com a necessidade de uso dos núcleos. De forma automática, ela permite que os núcleos do processador trabalhem mais rápido que a frequência básica de operação quando estiverem operando abaixo dos limites especificados para energia, corrente e temperatura. A tecnologia Intel Turbo Boost é ativada quando o sistema operacional (SO) solicita o estado de desempenho mais elevado.

A frequência máxima da tecnologia Intel Turbo Boost depende do número de núcleos ativos. O tempo que o processador gasta no estado da tecnologia Turbo Boost depende da carga de trabalho e do ambiente operacional, proporcionando o desempenho de que você precisa, quando e onde for necessário. Os elementos que podem definir o limite superior da tecnologia Turbo Boost em uma determinada carga de trabalho são os seguintes: número de núcleos ativos, consumo estimado de corrente, consumo estimado de energia e temperatura do processador.

Quando o processador estiver operando abaixo desses limites e a carga de trabalho do usuário exigir desempenho adicional, a frequência do processador aumentará dinamicamente 133 MHz em intervalos curtos e regulares até ser alcançado o limite superior ou o máximo upside possível para o número de núcleos ativos. Por outro lado, quando algum desses limites for alcançado ou ultrapassado, a frequência do processador cairá automaticamente 133 MHz até que ele volte a operar dentro dos seus limites.

O modo Turbo Boost explora a economia de energia através do aumento de frequência de um único núcleo, caso necessário. Esta ação corrobora com a preocupação da Intel em sempre melhorar a performance das aplicações usadas hoje em dia. Como boa parte das aplicações hoje em dia ainda não são multithreaded, de forma que tirem o maior proveito de Hyper-Threading, o 'overclocking' do modo Turbo irá fazer com que estas aplicações sejam executadas em menos tempo.

5. QUICKPATH INTERCONNECT

Uma importante mudança no projeto da CPU foi a troca do antigo barramento FSB (Front Side Bus), que compartilhava acessos entre a memória e a I/O, pelo novo barramento QPI (QuickPath Interconnection), que é projetado para aumentar a largura de banda e diminuir a latência.

O QPI utiliza dois caminhos para a comunicação entre a CPU e o chipset, como pode ser visto na Figura 2. Isto permite que a CPU faça a operação de transmissão e recepção dos dados de I/O ao mesmo tempo, isto é, os datapaths de leitura e escrita para esta função são separados. Cada um destes caminhos transferem 20 bits por vez. Destes 20 bits, 16 são utilizados para dados e os

restantes são usados para correção de erro CRC (Cyclical Redundancy Check), que permite ao receptor verificar se os dados recebidos estão intactos.

Além disso, o QPI trabalha com uma frequência de 3.2 GHz transferindo dois dados por ciclo (uma técnica chamada DDR, Double Data Rate), fazendo o barramento trabalhar como se estivesse operando a uma taxa de 6.4GHz. Como 16 bits são transmitidos por vez, tem-se uma taxa teórica máxima de 12.8 GB/s em cada um dos caminhos. Comparado ao FSB, o QPI transmite menos bits por ciclo de clock mas opera a taxas muito maiores. Uma outra vantagem em relação ao FSB, é que como o FSB atende às requisições de memória e de I/O, há sempre mais dados sendo transferidos neste barramento comparados ao QPI, que atende apenas às requisições de I/O. Por isso, o QPI fica menos ocupado, e assim, maior largura de banda disponível. Por último, o QPI utiliza menos ligações do que o FSB

Uma característica incorporada ao QPI são os modos de energia que ele pode assumir chamados de L0, L0s e L1. O L0 é o modo no qual o QPI está em funcionamento pleno. O estado L0s indica os fios de dados e os circuitos que controlam estes fios estão desativados para economia de energia. E em L1 todo o barramento está desativado, economizando ainda mais energia. Naturalmente, o estado L1 necessita de um tempo maior para reativação do que o L0s.

Existe também uma técnica introduzida para aumentar a confiabilidade do QPI. O QuickPath permite que cada caminho de 20 bits ainda seja dividido em outros quatro de 5 bits. Esta divisão melhora a confiabilidade principalmente em ambientes servidores.

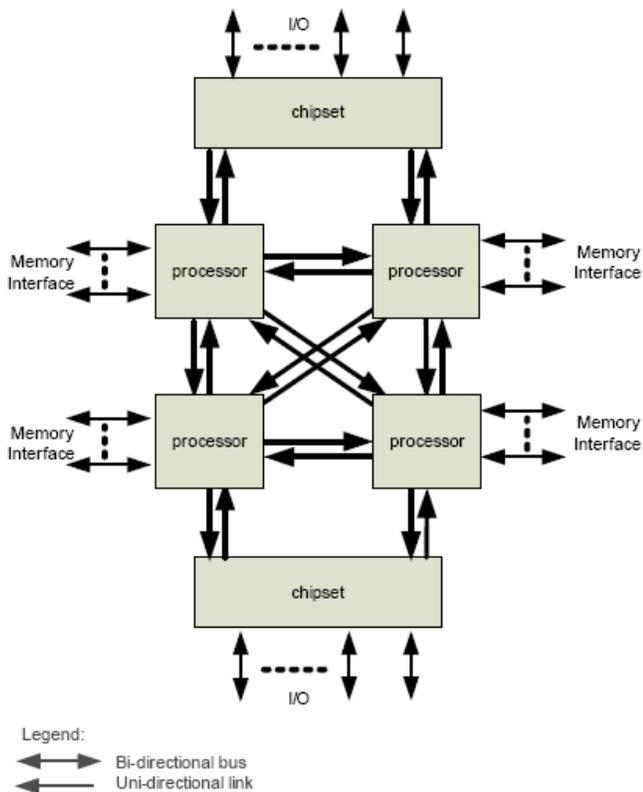


Figura 3. QuickPath Interconnect da Intel.

Quando esta funcionalidade é implementada, o receptor de dados pode perceber que a conexão entre ele e o transmissor foi danificada, e assim, desativar a porção do barramento que foi danificada e operar com a transmissão de menos bits por vez. Isto diminui a taxa de transmissão mas por outro lado o sistema não falha.

5.1 Comunicação em Camadas

Teoricamente, o barramento QPI deveria ser chamado de uma conexão ponto-a-ponto, pois conecta apenas dois dispositivos. Entretanto, vale ressaltar que os dados são enviados em paralelo através das várias conexões ponto-a-ponto existentes.

Assim como se faz em redes de computadores, a comunicação do barramento é feita por pacotes, que são quebrados em múltiplas transferências que ocorrem em paralelo, e possui cinco camadas, descritas brevemente a seguir:

- física: são os próprios fios que transportam o sinal, assim como o circuito e lógica necessários para realizar a transmissão e recebimento de 0s e 1s. A unidade de transferência na camada física é de 20 bits, chamada de Phit (Physical Unit).
- de enlace: responsável por tornar confiável a transmissão e o fluxo de controle.
- de roteamento: decide o caminho a ser percorrido pelo pacote na malha.
- de transporte: possui uma avançada capacidade de roteamento para que a transmissão fim-a-fim seja confiável.
- de protocolo: conjunto de regras de alto nível para a troca de pacotes de dados entre os dispositivos.

5.2 Coerência de Cache

Uma outra característica importante do QPI é a implementação de um protocolo de monitoração para manter a coerência de cache entre todos os controladores de cache no Core i7. O protocolo utilizado é uma versão modificada do conhecido protocolo MESI com a introdução de um novo estado F (forward). Este estado foi introduzido a fim de permitir a limpeza de linhas de encaminhamento de cache para cache. As características de todos estes estados estão resumidas na tabela a seguir.

Tabela 1. Os estados da cache no protocolo MESIF.

Estado	Limpo /Sujo	Pode Escrever?	Pode Encaminhar?	Pode Mudar para...
M-Modificado	Sujo	Sim	Sim	-
E-Exclusivo	Limpo	Sim	Sim	MSIF
S-Compartilhado	Limpo	Não	Não	I
I-Inválido	-	Não	Não	-
F-Encaminhar	Limpo	Não	Sim	SI

6. GERENCIAMENTO DE MEMÓRIA

Com a controladora de memória dentro do processador, os núcleos não devem percorrer o longo caminho do FSB cada vez que necessitarem um dado da memória RAM. Aproveitando a ocasião da inclusão de vários núcleos (2, 4 ou mais) no mesmo chip, a Intel optou por implementar uma controladora de memória com 3 canais. Com uma largura efetiva de 192 bits e usando memórias DDR3 (apenas, memórias DDR2 não são suportadas), a oferta de banda de memória atinge níveis bem maiores que os convencionais.

A integração de 4 núcleos (com possibilidade para mais núcleos, conforme a necessidade/possibilidade por questões energéticas/térmicas) no mesmo chip, requer uma reorganização na estrutura de cache. O grande cache L2 compartilhado do Core2 funciona muito bem quando há apenas 2 núcleos por chip, mas 4 núcleos disputando acesso ao cache L2 pode e tronar um gargalo. Então, transportou-se o cache compartilhado para um nível superior e entre eles criou-se um cache L2; razoavelmente pequeno, mas de latência baixíssima (para um cache L2), para diminuir a concorrência pelo grande cache L3, de 8MB; compartilhado por todos os núcleos.

Os caches dos Core2 e Nehalem são organizados de forma inclusiva. Assim, cada nível superior guarda uma cópia do nível anterior. O cache L2 de cada núcleo possui uma cópia do cache L1 e o cache L3 guarda uma cópia de cada cache L2; portanto, dos 8MB, sobram efetivamente 7MB (já que 1MB é reservado para cópia dos quatro caches L2 de 256KB). Este sistema requer cuidados para que seja mantida a consistência dos dados; pois cada vez que um cache é atualizado, suas cópias também devem ser atualizadas. Porém, facilita o compartilhamento de dados entre os núcleos, já que todos os dados presentes nos caches L1 e L2 de todos os núcleos são encontrados no cache L3.

O cache L2 é exclusivo e de comportamento chamado "victim-cache", pois só recolhe as "vítimas" do cache L1 (dados eliminados por falta de espaço). O cache L3 também é um "victim-cache", mas não é inclusivo nem exclusivo. Não guarda cópias dos demais caches, mas permite o compartilhamento de dados. Se mais de um núcleo precisar de um mesmo dado, é mantida uma cópia no cache L3 e esta é marcada com uma flag de compartilhamento para que não seja apagada por já constar em outros níveis superiores. A vantagem deste sistema é que quando um núcleo requisitar um dado à controladora de memória, este "sobe" diretamente ao cache L1, enquanto os outros caches se reorganizam, abrigando as vítimas dos níveis superiores. Porém, antes disso, cada núcleo deve requisitar aos demais se já possuem em cache o dado em questão, antes de pedi-lo à controladora de memória. Se algum núcleo o tiver, pode enviar a outro núcleo pelo crossbar e uma cópia é guardada no cache L3.

Dois aspectos importantes da estrutura de cache da Intel são a garantia de muita banda e latências excelentes. A latência do cache L1 teve que aumentar de 3 para 4 ciclos, devido à implementação do SMT (Hyper Threading) já que ambos núcleos virtuais compartilham o mesmo cache L1. Mas a latência do cache L2 caiu consideravelmente, dos 23 ciclos do cache L2 do "Penryn" (Core2 de 45nm) para apenas 10 ciclos. O cache L3 é um caso à parte, como se encontra em outra região do processador (na parte "uncore" da figura 1, onde ficam também a controladora

de memória e o controlador do QPI), que segue um clock próprio e tem relação com o clock da memória; mas também é muito rápido. E a controladora de memória é especialmente eficiente, obtendo altíssimas taxas de transferência mesmo em condições pouco favoráveis, como utilizando memórias DDR3 de clock relativamente baixo (DDR3-1066, por exemplo).

7. CONCLUSÃO

Esta análise sobre as principais características que fazem do Core i7 um processador diferenciado mostrou como a indústria dispõe aos consumidores uma vasta gama de novas funções visando o ganho de desempenho em uma curta janela de tempo. Seja pelo uso do Turbo Boost, que utiliza lógica para otimizar o consumo de energia; seja pelo QPI, uma conexão ponto-a-ponto de alta velocidade, a Intel conseguiu atacar de forma abrangente os principais problemas que concernem ao multicore. Outro aspecto relevante a ser mencionado aqui é a volta do Hyper-Threading corroborando com a afirmação de que na computação algumas abordagens são recorrentes.

Mais importante do que as inovações que o Core i7 proporcionou é a consolidação de uma era na indústria que é voltada ao design com a replicação de núcleos dentro do processador, iniciada com a geração do Core Duo. Os ganhos em desempenho já obtidos em relação aos Core Duo de até 30% são apenas uma amostra do potencial deste quad-core: os ganhos poderão ser efetivamente notados quando boa parte das aplicações forem voltadas para este tipo de processador.

8. REFERÊNCIAS

- [1] Intel® Core™ i7 Processor Extreme Edition Series and Intel® Core™ i7 Processor Datasheet - Volume 1. Document # 320834-002. Acessado em 02/07/2009 em <http://www.intel.com/design/corei7/documentation.htm>
- [2] Intel® Core™ i7 Processor Extreme Edition Series and Intel® Core™ i7 Processor Datasheet - Volume 2. Document Number: 320835-002. Acessado em 02/07/2009 em <http://www.intel.com/design/corei7/documentation.htm>
- [3] An introduction to Intel® QuickPath Interconnect white paper. Document Number: 320412-001US. Acessado em 02/07/2009 em <http://www.intel.com/technology/quickpath/introduction.pdf>
- [4] Intel® Turbo Boost Technology in Intel® Core™ Microarchitecture (Nehalem) Based Processors. Acessado em 02/07/2009 em <http://www.intel.com/portugues/technology/turboboost/index.htm>
- [5] Stallings, William, Arquitetura e Organização de Computadores. Editora Prentice Hall, Quinta Edição, 2003.
- [6] Intel® Turbo Boost Technology in Intel® Core™ Microarchitecture (Nehalem) Based Processors. Acessado em 02/07/2009 em http://download.intel.com/design/processor/applnots/320354.pdf?iid=tech_tb-paper