Computerarchitectuur

Roel Van Steenberghe

Table of Contents

Over deze cursus v
Voorwoord vi
1. power supply 1
1.1. Principe en werking 1
1.2. Eigenschappen 2
1.3. Vormfactor en connectoren 2
1.4. Vermogen 3
1.5. Geluid 4
1.6. Rendement 4
1.7. Problemen 5
1.8. Uninterruptible Power Supply (UPS) 6
1.8.1. Online UPS 7
1.8.2. Offline UPS 7
1.8.3. Line-interactive UPS 8
1.9. Accu's 8
1.9.1. Belangrijke parameters 9
2. CPU 12
2.1. Overzicht 12
2.2. Technologie en functionaliteit 13
2.3. Kloksnelheid 15
2.4. Processorarchitectuur 16
2.4.1. Pipelining 16
2.4.2. Superscalaire processoren 17
2.4.3. Cache 20
2.5. APU, SoC 21
2.6. Montage 21
2.7. Processoren van de toekomst 23
2.8. Bibliografie bij dit hoofdstuk 23
3. Algemene bibliografie 24

List of Figures

1.1. Principe schakelende voeding 1
1.2. Rack-mountable UPS (bron: www.apc.com) 6
1.3. Online UPS (© GFDL Joslee 2007) 7
1.4. Offline UPS (© Joslee 2007 GFDL) 8
1.5. Line interactive UPS (© Joslee 2007 GFDL) 8
1.6. accu 9
2.1. Wet van Moore (CC, Wikimedia Commons) 14
2.2. Intel roadmap (copyright 2008-2012 WhiteTimberwolf GFDL) 15
2.3. processor pipeline (CC mediawiki) 17
2.4. Sandy bridge microarchitectuur 18
2.5. AMD bulldozer architectuur (copyright AnandTech) 19
2.6. single threaded applicatie op multicore processor 20
2.7. LGA2011 socket zonder processor 22

List of Tables

1.1. 80 plus certificatie (bron: Wikipedia) 5
2.1. processoroverzicht 12

Over deze cursus

Deze cursus werd opgesteld doorheen de jaren, met wisselende auteurs. Elk van hen ben ik uiteraard dankbaar, specifiek Dhr Sven Sanders Dhr Johan Donne die de fundamenten van deze informatiebron reeds jaren geleden gelegd hebben.

Er werd in deze cursus gepoogd om steeds correct om te gaan met extern bronmateriaal. Mocht je toch een stukje materiaal zonder correcte bronvermelding, dan passen we dat uiteraard ook meteen aan.

Door deze cursus in bronvorm aan te bieden op Github is er ook de hoop dat er ook door anderen toevoegingen kunnen gebeuren. Hergebruik van het materiaal is dan ook toegelaten, maar wel onder voorwaarden:

- het materiaal mag niet commercieel beschikbaar gesteld worden zonder uitdrukkelijke en schriftelijke toestemming van de auteur
- het materiaal aanpassen mag, maar dan op voorwaarde dat de aanpassingen ook publiek beschikbaar worden gesteld. Bij voorkeur gebeurt dit via deze weg, zodat iedereen mee kan genieten van de verbeteringen

Concreet betekent dit dat al het materiaal onder de Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 4.0 Internationaal-licentie[1] valt.

Wie correcties of aanvulling aanbrengt in deze cursus, zal een vermelding krijgen op deze pagina.

[1] http://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl

Voorwoord

Als iemand van de buitenwereld je de komende jaren vraagt wat je precies gestudeerd hebt, of wat je doet als werk, dan zal je antwoord vaak 'iets met computers' zijn. Soms is dat nu eenmaal de makkelijkste manier om je er vanaf te maken. Voor veel mensen zijn computers, tablets, smartphones en andere devices tegenwoordig zo gewoon, dat ze bijna thuis horen in het rijtje van basisbehoeften als stromend water, elektriciteit en TV. Toch blijft het belangrijk om te weten wat er onder de motorkap van je devices schuilt. Die achtergrondkennis is onontbeerlijk om later efficiënt problemen op te lossen of producten (in de breedste zin van het woord) van goeie kwaliteit af te leveren. Zelfs wie zich later zal toespitsen op het ontwikkelen van software, zal efficiënter kunnen werken als hij ook snapt wat achter de schermen gebeurt. Deze cursus probeert je een overzicht te geven van de interne keuken van een moderne computer terwijl de cursus processorarchitectuur dan weer iets dieper ingaat op de werking van het kloppend hart ervan. Uiteraard zijn twaalf lessen veel te weinig om alle onderdelen tot op het bot uit te benen. Daarom kan ik enkele standaardwerken aanbevelen, die zeker een bron van inspiratie vormden voor deze cursus. De boeken van William Stallings [STALLINGS] en Umakishore Ramachandran [RAMA] verdienen zeker je aandacht. Een overzicht van de werkvorm die bij dit vak gebruikt wordt, vind je terug in de ECTS fiche en de studiewijzer. Beiden zijn te vinden op Toledo.

Veel succes met deze cursus!

Roel Van Steenberghe

Chapter 1. power supply

1.1. Principe en werking

Een computer, of het nu een pc, laptop, server of smartphone is, kan enkel functioneren als de juiste elektrische spanningen aangevoerd worden. Elektronische componenten vragen een relatief lage, maar erg stabiele gelijkspanning om te functioneren. Deze wordt geleverd door een voeding, die de wisselspanning van het elektriciteitsnet omzet naar de nodige gelijkspanningsniveau's. De techniek die hierbij gebruikt wordt noemt men switched mode power supply of geschakelde voeding. Het schema van de omzetting wordt weergegeven in onderstaande afbeelding

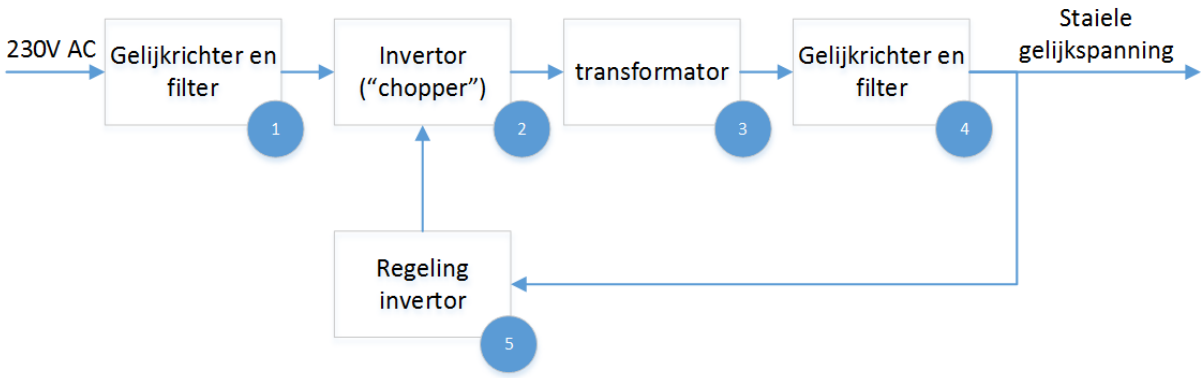

Figure 1.1. Principe schakelende voeding

Een eerste stap ① is de gelijkrichter aan de ingang, waarmee de wisselspanning wordt omgezet naar een gelijkspanning. Deze gelijkspanning wordt vervolgens gefilterd, zodat de variatie in het spanningsniveau beperkt wordt. De tweede stap ② is een stuk minder voor de hand liggend. Op basis van de gelijkgerichte en gefilterde ingangsspanning zal een invertor een blokgolf genereren. Deze wisselspanning wordt bekomen door het aan- en afschakelen van de ingangsspanning. Eigenlijk is de combinatie van de eerste twee stappen samen te vatten als een frequentieomvormer. Het ingangssignaal wordt omgezet naar een hoger-frequent signaal (van 50Hz naar frequenties boven 20kHz).

Het voordeel van deze omzetting is dat de transformator in de volgende stap een stuk kleiner en efficiënter kan zijn. Deze gelijkrichter en transformator ③ brengt de spanning naar het gewenste niveau, waarna het met de uitgangs-gelijkrichter en filter ④ wordt omgezet naar een stabiele gelijkspanning.

In de figuur is ook te zien dat de uitgangsspanning teruggekoppeld wordt ⑤ naar de invertor. Op die manier kan de uitgangsspanning nog geregeld worden. De invertor-stap heeft immers ook invloed op de amplitude van zijn uitgang. Deze terugkoppeling gebeurt meestal met optocouplers om een galvanische scheiding te bekomen.

Om het verbruik van een CPU uit te drukken, wordt vaak gesproken over TDP. Dat is een waarde die aanduidt hoeveel energie de CPU maximaal dissipeert. Echter dient opgemerkt te worden dat *AMD* en *Intel* hiervoor verschillende berekeningsmethodes gebruiken. De TDP geeft dus een indicatie over het maximale verbruik, maar gedetailleerde benchmarks blijven nodig om exacte waarden te kennen.

1.2. Eigenschappen

1.3. Vormfactor en connectoren

De eerste (IBM) PC beschikte over een moederbord met AT vormfactor, de bijhorende voeding was dan ook een AT voeding. In 1995 kwam er een opvolger, met name de ATX vormfactor. Ondertussen is deze specificatie ook geëvolueerd (ondertussen ATX 2.3). De belangrijkste verschillen situeren zich op het vlak van de spanningen die de voeding kan afgeven en de connectoren die voorzien zijn op de voeding. In het bijzonder is er natuurlijk een verschil tussen de verschillende connectoren die op het moederbord worden aangesloten. Een AT voeding bood een connector van tweemaal zes aansluitingen, een ATX voeding biedt daarentegen een connector met 20 aansluitingen. Een belangrijk verschil tussen beiden is de aanwezigheid bij ATX van een 3.3V spanning, een +5V standby en power on signaal. Deze laatste twee maken het mogelijk dat de mechanische schakelaar van de AT voeding (die rechtstreeks de voeding aanstuurde), vervangen kon worden door een elektronisch signaal van het moederbord naar de voeding. In eerste instantie kan het moederbord dit signaal sturen als het zelf een input krijgt van een drukknop. Er zijn echter ook alternatieven mogelijk, zoals wake-on-lan, speciale toetsen op een toetsenbord, ... Hieruit kan je afleiden dat bij een computer die uitgeschakeld is, een deel van het moederbord nog steeds onder spanning staat. Deze spanning kan je alleen wegnemen door de voeding uit te schakelen (schakelaar op voeding, stekker uittrekken). Naast de verschillen in connectoren die op het moederbord worden aangesloten, is er ook onderscheid op het vlak van de andere connectoren.

Afhankelijk van de andere apparaten (en hun voedingsaansluiting), moet je erop letten om een voeding te kiezen die de nodige connectoren aanbiedt.

Enkele belangrijke connectoren zijn:

- Moederbordconnector: afhankelijk van vormfactor
- 4-pin connector (molex): o.a. voor (ATA) schijven, optische drives
- SATA voedingsconnector
- Auxillary connectors: verschillende varianten van extra voedingsconnector en om extra vermogen te leveren
- PCI-express connector

1.4. Vermogen

Een erg belangrijke eigenschap voor een voeding is het vermogen dat ze kan leveren. Uiteraard moet dit te leveren vermogen voldoende zijn om alle componenten in het systeem te voorzien van stroom. Het vergelijken van voedingen op dit vlak is iets complexer dan kijken naar de waarden die de fabrikant op zijn verpakking adverteert. Belangrijker dan het getal is de betekenis ervan. Aangezien er geen voorschriften zijn voor de bepaling van die vermogenswaarde, kan 500W bij de ene fabrikant betekenen dat de voeding 500W piekvermogen kan leveren bij 10°C en bij een andere een continu vermogen van 500W bij 40°C. Als het systeem continu 450W nodig heeft, zou de eerste voeding kunnen falen. Een tweede belangrijke opmerking is dat niet alleen het totale vermogen belangrijk is, maar ook het vermogen dat op elke voedingsspanning apart geleverd kan worden. Het is duidelijk dat een computervoeding meerdere eindtrappen moet bevatten voor de verschillende spanningen. Op elk van deze rails is er een maximale stroom die geleverd kan worden. Als de maximale stroom op de 12V rail 5A is, kan je met een 500W voeding niet voorzien in de behoeften van een computer die een vermogen van 200W nodig heeft, maar wel 6A op de 12V rail. Dit kan een belangrijke reden voor prijsverschillen in voedingen zijn. Goedkopere voedingen kunnen typisch meer stroom leveren bij de lagere spanningen en minder bij 12V. Er moet nog worden opgemerkt dat sommige voedingen verschillende rails hebben voor eenzelfde voedingsspanning. Op elk van deze rails is dan een maximale stroom vastgelegd. Het zal wel duidelijk zijn dat je dan best de verbruikers op een zo evenwichtig mogelijke manier over deze rails moet verdelen. Een laatste opmerking is dat het vermogen van de voeding zo goed mogelijk op het systeem moet worden afgestemd. Uiteraard betekent dit dat je voldoende piekvermogen nodig hebt,

maar zomaar een voeding van 1kW aanschaffen voor een systeem dat 200W nodig heeft is niet meteen een goede keuze.

1.5. Geluid

De geluidsproductie van een computer is in verschillende gebruiksomgevingen liefst zo klein mogelijk. Een belangrijke bron van lawaai wordt gevormd door de verschillende koelingen en in het bijzonder de ventilatoren die hierbij worden gebruikt. Hier blijkt alvast het belang van het rendement van een voeding. Hoe hoger het rendement, des te minder verlies er is. Dit verlies manifesteert zich steeds onder de vorm van warmte. Meer warmteverlies betekent dus dat er nood is aan een groter koelvermogen. Naast het rendement is ook de grootte van de ventilator belangrijk. Een grotere ventilator zal bij lagere toerentallen voldoende kunnen koelen en daarbij minder lawaai produceren. Er bestaan ook voedingen die volledig passief (zonder ventilatoren) gekoeld worden. Deze produceren uiteraard geen lawaai, maar zijn typisch iets duurder.

1.6. Rendement

Het ‘groene’ aspect bij pc’s komt steeds meer naar voor. Het rendement van de voeding is daarbij een belangrijke factor. Je wil natuurlijk voor elke 100 Watt die je uit het stroomnet haalt, ook 100W prestaties zien. Helaas is dit niet mogelijk: voedingen hebben een rendement dat een stuk lager ligt dan de ideale 100%. Dat verlies uit zich voornamelijk in warmte, die dan weer moet afgevoerd worden. Het spreekt voor zich dan een hoger rendement meestal ook een iets hoger prijskaartje met zich zal meebrengen. Toch is dit het overwegen waard als je een kleine rekenoefening maakt. Een computer met scherm die niet erg zwaar belast verbruikt ongeveer 200 Watt. Als je deze pc elke werkdag 10 uur gebruikt, dan komt het verbruik op 0,150 kW x 10 uur per dag x 250 werkdagen= 375 kWh per jaar Als je daar de prijs tegenover zet die een gemiddeld gezin (bron: VREG, oktober 2012) betaald per kWh, dan kost deze pc je 375 * 0,2€ = € 75. Een voeding met een rendement dat 20% beter is zal je dus op jaarbasis makkelijk 15 Euro opleveren. Het loont dus de moeite om bij de aankoop de voeding zorgvuldig te kiezen. In een bedrijf met honderden desktops begrijp je dat dit een verkoopsargument kan zijn.

Het 80-plus certificatieprogramma probeert voor de consument duidelijkheid te scheppen door voedingen een label te geven naargelang de efficiëntie. De certificatie is echter geen verplichting voor fabrikanten.

Table 1.1. 80 plus certificatie (bron: Wikipedia[1])

	standaard	brons	zilver	goud	platinum	titanium [a]
20% belast	>=80%	>=82%	>=85%	>=87%	>=90%	>=94%
50% belast	>=80%	>=85%	>=88%	>=90%	>=92%	>=96
100% belast	>=80%	>=82%	>=85%	>=87%	>=89%	>=94

[a] bij titanium worden ook nog extra eisen gesteld

Laptops hebben een verbruik dat typisch een flink stuk lager zit. Hoewel ze een voeding hebben die meestal een behoorlijk hoog wattage aankan om de accu op te laden, is het gemiddeld verbruik meestal slechts rond de 30Watt. Het matige rendement van PSU's is voor een deel eigen aan de opbouw ervan. Omdat veel verschillende eindtrappen nodig zijn voor de verschillende spanningen, is het totale rendementsverlies een accumulatie van de kleinere verliezen bij de deeltrappen. Ondertussen verlaten sommige grote spelers om die reden de ATX standaard om met eigen oplossingen hogere rendementen te behalen. Google ontwikkelt bijvoorbeeld z'n eigen servervoedingen die door hun eenvoud een veel hoger rendement halen. Google research publiceerde een paper [2] die schat dat de energiebesparing die je heermee kan behalen op een populatie van 100 miljoen computers 13 miljard kWh betreft op jaarbasis. Dat komt, om je een idee te geven, ongeveer overeen met de opbrengst van de helft van een kerncentrale zoals die in Doel (jaarproductie 22 miljard kWh)

1.7. Problemen

Problemen met voedingen hebben altijd gevolgen voor het volledige systeem, aangezien ze dit volledige systeem van stroom moeten voorzien. Een belangrijke oorzaak van problemen is een te klein vermogen voor het systeem of onvoldoende koeling. Dit probleem uit zich meestal niet in het niet opstarten van het systeem, maar eerder in het onverwacht afsluiten (of eventueel herstarten) ervan. Dit is dan nog het meest aangename gevolg van het probleem. Het is belangrijk om bij dergelijke problemen de voeding en de koeling ervan te controleren. Minder aangename gevolgen kunnen zijn dat de voeding beschadigd raakt en in het meer

[1] http://en.wikipedia.org/wiki/80_Plus

dramatische geval dat er rook uit de computerkast komt. Deze kan dan afkomstig zijn van de voeding zelf, maar ook van andere componenten(moederbord, RAM, CPU). Een situatie die de meesten liever vermijden. Een voeding kan ook slijtage vertonen. In het bijzonder op het vlak van de elektrolytische condensatoren kan er veel verschil zijn tussen voedingen. Minder kwalitatieve condensatoren kunnen uitdrogen (elektrolyt dat verdampt), waardoor ze hun functie minder tot niet meer vervullen en de voeding uiteindelijk rook in plaats van gelijkspanning produceert. Dit gebeurt uiteraard pas na verloop van tijd (afhankelijk van de belasting van de computer). Sommige voedingen hebben een controlesysteem dat je door middel van geluidssignalen preventief waarschuwt als er problemen dreigen, zoals overbelasting of een gebrekkige koeling.

1.8. Uninterruptible Power Supply (UPS)

Een UPS is een toestel dat het wegvallen van de netspanning kan opvangen. Hiervoor bestaat een UPS uit een accu en een elektronische schakeling die de accuspanning kan omzetten naar een netspanning.

Figure 1.2. Rack-mountable UPS (bron: www.apc.com[2])

Bij het wegvallen van de netspanning zal de UPS ogenblikkelijk de stroomvoorziening over nemen. Voor de aangesloten toestellen treedt er dus geen onderbreking op. Een UPS kan de stroom natuurlijk niet onbeperkt in de tijd overnemen. Hoe lang de UPS dit kan volhouden, hangt af van de

[2] http://www.apc.com

accu's en het gevraagde vermogen. Om te vermijden dat apparatuur plotseling en ongecontroleerd stilvalt, heeft een UPS dikwijls ook een interface naar de computer. Deze laat toe dat de UPS de computer 'proper' afsluit op het ogenblik dat de accu-stroom een bepaalde ondergrens bereikt. Een alternatief kan erin bestaan dat de UPS gecombineerd wordt met een dieselgenerator. De UPS zorgt dan voor de ogenblikkelijke overname van de stroomvoorziening en geeft de generator de nodige tijd om op te starten. Zodra de generator actief is, neemt deze de stroomvoorziening op zich. Een UPS heeft meestal ook een spanningsbeveiliging aan boord die je apparatuur kan beschermen tegen storingen op het elektriciteitsnet. UPS'en vind je in alle prijsklasses, wat vaak te maken heeft met de inwendige opbouw ervan. Er onderscheiden zich enkele grote types.

1.8.1. Online UPS

De online UPS wordt ook wel "double conversion" ups genoemd. Alle stroom die naar de IT-apparatuur gaat, loopt door de UPS. Hierdoor is het niet nodig om te schakelen bij het uitvallen van de stroom. Met de bypass kan je evenwel de ups overbruggen. Dat kan bijvoorbeeld interessant zijn als er onderhoud nodig is. Omdat hierdoor veel gevraagd wordt van alle elektronica (die constant volledig belast wordt), is die een relatief duur concept.

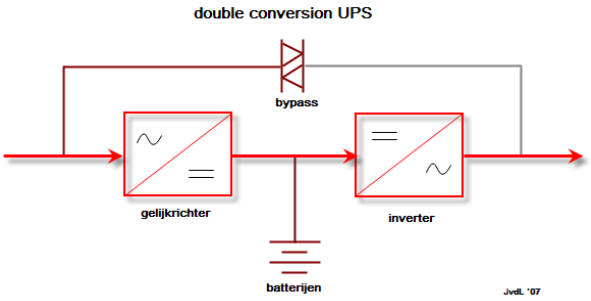

Figure 1.3. Online UPS (© GFDL Joslee 2007)

1.8.2. Offline UPS

Dit type UPS vind je voornamelijk terug bij particuliere ups'en waar kostprijs een belangrijk criterium is. Bij het wegvallen van de spanning, wordt een bypass ingeschakeld. Die procedure duurt enkele milliseconden waarbij je geen uitgangsspanning hebt, en dat moet opgevangen worden door de voeding van je computer of server. Een nadeel van dit type UPS is dat je hem ook niet zonder risico kan testen. Ander nadeel is dat in gewone omstandigheden de netspanning

rechtstreeks gekoppeld is aan je IT-apparatuur. Als er storingen op het net zitten, zal je IT apparatuur daar hinder van ondervinden. De apparatuur is dus niet beveiligd.

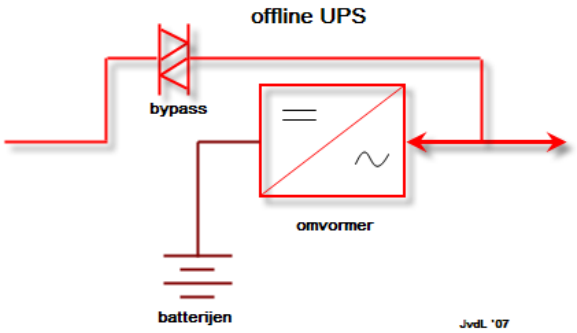

Figure 1.4. Offline UPS (© Joslee 2007 GFDL)

1.8.3. Line-interactive UPS

Deze vorm van UPS vormt een hybride oplossing. In feite gaat het om een off-line UPS waar de line-feed voorzien is van aanvullende filters. Zo ben je zeker dat de spanning die aan je servers aangelegd is, gezuiverd werd van pieken en storingen. In omgevingen waar veel storing optreedt is dat geen overbodige luxe. (bijvoorbeeld fabriekshallen, gebieden met gebrekkige stroomvoorziening)

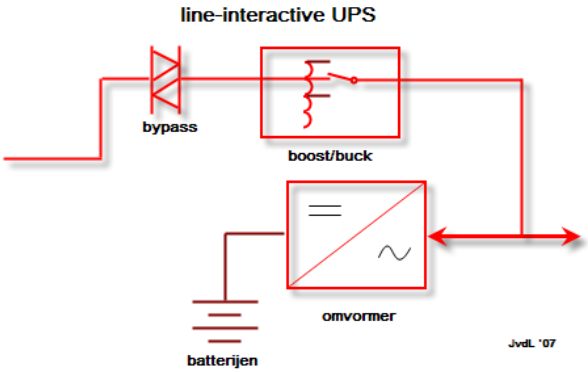

Figure 1.5. Line interactive UPS (© Joslee 2007 GFDL)

1.9. Accu's

Tegenwoordig kunnen we het niet meer hebben over computervoedingen zonder even uit te wijden over accu's. In de trend naar mobiliteit (laptops, tablets, smartphones), vormen die een onmisbare schakel.

1.9.1. Belangrijke parameters

Capaciteit

De capaciteit van batterijen wordt meestal uitgedrukt in Ah (ampère/uur) of mAh (milliampère/uur). Met die eenheid kan je makkelijk accu-packs vergelijken. Een batterij van 6Ah zal bijvoorbeeld in staat zijn om gedurende 6 uur een stroom af te leveren van 1 Ampère, of gedurende bijvoorbeeld 2 uur een stroom van 3 Ampère. Sommige fabrikanten verkiezen echter om hun capaciteiten uit te drukken in Wh, wat vergelijken moeilijk kan maken. Toch kan je eenvoudig omrekenen: Je weet immers dat

P=U*I (Vermogen=Spanning x Stroom)

Willen we dus de stroom I(A) kennen, dan moeten we het vermogen delen door de spanning. Nemen we onderstaand voorbeeld:

Figure 1.6. accu

We kunnen hier dus de capaciteit in Ah bepalen door I_h = P_h/U = 2,4Wh/3,6V = 0,666Ah of 666mAh

Aantal cellen

Een accu wordt opgebouwd uit verschillende cellen. Bijvoorbeeld bij Li-ion accu's kunnen die elk ongeveer 3V leveren. Het spreekt voor zich dat een toename van het aantal cellen zal betekenen dat de totale capaciteit ook toeneemt. Oefenvragen: Wat is de capaciteit van je eigen laptopaccu? Stel dat je deze accu gebruikt om een lamp te doen branden die 5Watt verbruikt. Hoe lang zal de lamp branden? Uit hoeveel cellen bestaat je accu-pack?

Laadcurve

Om de optimale kwaliteit van de accu te garanderen over langere termijn is het nodig om de juiste laadcurve te respecteren. Een batterij zal uiteraard stroom nodig hebben om zich op te laden, maar het is niet noodzakelijk zo dat een hogere stroom zal betekenen dat de batterij sneller oplaadt. Het gebruik van de juiste en kwalitatieve adapter is hierbij erg belangrijk.

Memory-effect

Het memory-effect is een term die vaak gebruikt wordt om aan te geven dat bepaalde types batterijen, met NiCd op kop, vaak een effect vertonen waarbij het lijkt dat de batterijen snel hun capaciteit verliezen als je ze halverwege de ontlaadcyclus terug oplaadt. Dat fenomeen is eigenlijk de verzamelnaam van effecten die worden veroorzaakt door een combinatie van elektrische en chemische processen.

LI-ION accu's

Tegenwoordig is dit zowat het meest voorkomende type in hoogwaardige mobiele apparatuur. Dit type onderscheidt zich door een erg hoge energiedichtheid, en het 'memory-effect' is niet bestaande.

Toch zijn er enkele belangrijke eigenschappen aan dit type, die je beter kent.. Het zwakke punt van Li-Ion: degradatie Wie een laptop of GSM gebruikt, kent het fenomeen: na enkele jaren is de cyapaciteit van de batterij slechts nog een fractie van wat ze was bij aankoop. Dit fenomeen kan je niet omkeren, maar het kan wel vertraagd worden als je de weet wat de factoren zijn die dit proces versnellen... Een Li-ion-accu verliest zijn capaciteit het snelst als hij zich in een warme ruimte bevindt, en opgeladen is. Een volledig opgeladen Li-ion accu zal bijvoorbeeld na een jaar rusten in een ruimte waar het gemiddeld 20°C is, 20 procent van zijn capaciteit verliezen. Is diezelfde accu slechts half opgeladen, dan zal de capaciteit met slechts enkele procenten dalen. Het is dus niet verstandig aan Li-ion-accu voor lange tijd weg te bergen in opgeladen toestand. Ook door stockage in koele ruimtes kan de capaciteit langer bewaard blijven. Een laptop die snel erg warm wordt bij gebruik zal dus meteen ook nefast zijn voor de capaciteit van de batterij op langere termijn. Bij een temperatuur van iets boven het vriespunt en een lading van ongeveer 40% zal dit type batterij de langste levensduur 'on the shelf' hebben.

Toekomstige ontwikkelingen

Gezien de enorme markt die ontstaan is voor accu's, is er enorm veel druk om betere modellen te ontwikkelen. Daarbij worden bestaande types geperfectioneerd, maar ook nieuwe types ontwikkeld. Zo zijn er de LiPo (Lithium polymeer) batterijen die ongeveer 50% efficiënter zijn dan klassieke Li-Ion equivalenten, en ook de brandstofcellen (fuel cells) die mogelijks een oplossing kunnen vormen voor de steeds grotere autonomie-behoefte van toestellen. Omdat veel van deze technieken gebruik maken van erg zeldzame delfstoffen, komen ook geavanceerde technieken met courante materialen in het vizier ter optimalisatie of vervanging, zoals nanostructuren met koolstof. Deze blijven echter toekomstmuziek voor consumentenelektronica...

Chapter 2. CPU

2.1. Overzicht

In onderstaande tabel worden een aantal processoren van de x86 familie weergegeven met hun belangrijkste eigenschappen. De processor die in de eerste (IBM-)PC werd gebruikt was een 8088. Eigenlijk was dit een 8086 waarvan de databus beperkt werd tot 8 bits in plaats van 16 bits. De enige reden hiervoor was dat op dat ogenblik er geen andere 16bit componenten beschikbaar waren. Deze processor werd reeds uitgebreid besproken tijdens computertechniek. Het is niet de bedoeling om hier terug te komen op programmeermodel, segmentering, ...

Wel zullen we de evolutie van een aantal eigenschappen bekijken.

Table 2.1. processoroverzicht

type	jaar	data/ adres-bus	L1 cache (kB)	FSB (Mhz)	Clock(Mhz)	transistoren (miljoen)	technologie (nm)
8088	1979	8/20	-	4,77..8	4,77..8	0.029	3000
8086	1978	16/20	-	4,77..8	4,77..8	0.029	3000
80286	1980	16/24	-	6..20	6..20	0.134	1500
80386DX	1985	32/32	-	16..33	16..33	0.275	1500
80486DX/ SX	1989	32/32	8	25..50	25..50	1.2	1000
80486DX2	1992	32/32	8	25..40	25..80	1.2	800
80486DX4	1994	32/32	8+8	25..40	75..120	1.2	600
Pentium	1993	64/32	8+8	60..66	60..200	3	600
Pentium MMX	1997	64/32	16+16	66	166..233	4.5	350
Pentium Pro	1995	64/36	8+8	66	150..200	5.5	350
Pentium II	1997	64/36	16+16	66/100	300..450	7.5	250
Pentium III	1999	64/36	16+16	100/133	450..1300	28	130

type	jaar	data/ adres-bus	L1 cache (kB)	FSB (Mhz)	Clock(Mhz)	transistoren (miljoen)	technologie (nm)
AMD Athlon	1999	64/36	64+64	200/266	500..2200	37	130
Pentium IV	2001	64/36	8+96	400/533	1400..2800	42	130
AMD 64	2005	64/36	2*512k L2	2000	2,4GHz	233	102
Core duo	2006	64/36	2*2M L2	800	3,6GHz	376	65
Intel Nehalem	2008	64/36	32+32/ core	-	3,2 Ghz	731 (QC)	45/32
Intel Sandy Bridge	2011	64/36	32+32/ core	-	3,8 Ghz.[a]	995 (QC)	32
Intel Ivy bridge	2012	64/36	32+32/ core	-	3,9 Ghz.[a]	1400 (QC)	22
Intel Haswell	2013	64/36	32+32/ core	-	3,9 Ghz.[a]	1400	22

[a] deze waarden zijn niet continue en kunnen pas tijdelijk gehaald worden

2.2. Technologie en functionaliteit

Een eerste duidelijke evolutie is de toename van het aantal transistors. Volgens de wet van Moore verloopt deze stijging zelfs exponentieel. Elke vierentwintig maanden zou het aantal transistors in een processor verdubbelen . Die toename is uiteraard enkel mogelijk als de transistordichtheid kan toenemen. In het verleden werd hierbij vaak gedacht dat er technische beperkingen zouden opduiken, maar tot dusver blijven fabrikanten slagen om vast te houden aan de ontwikkelsnelheid die geponeerd werd door Gordon More, één van de oprichters van Intel.

> The number of transistors incorporated in a chip will approximately double every 24 months
>
> — Gordon Moore *Electronics Magazine 1965*

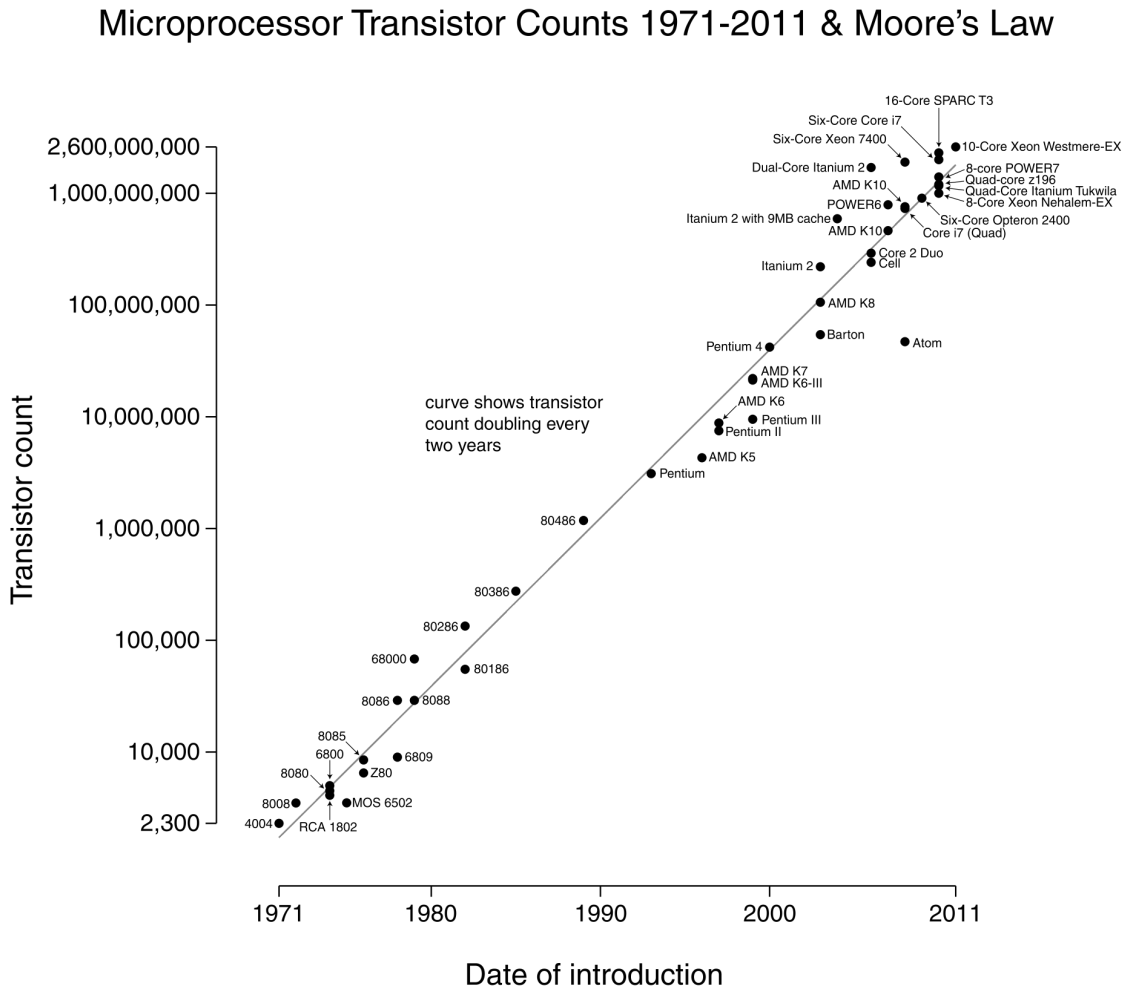

Figure 2.1. Wet van Moore (CC, Wikimedia Commons)

Met deze stijging van het aantal transistoren gaat uiteraard ook een toename in functionaliteit gepaard. Zo kent een x86 processor vanaf de 80286/80386 (in principe vanaf de 286, praktisch vanaf de 386) twee werkingsmodi: real mode en protected mode. In real mode heeft de cpu dezelfde functionaliteit als een 8086. In deze compatibiliteitsmodus gedraagt hij zich met andere woorden als een snellere versie van de 8086. In protected mode krijgt de processor extra functionaliteit. De naam protected mode komt van de extra toevoegingen op het vlak van geheugenbescherming. Daarnaast ondersteunde de processor vanaf deze modus een aantal, vandaag onmisbare, extra mogelijkheden. Onder andere multitasking en virtueel geheugen zijn enkel mogelijk met een protected mode processor. Hier moet nog opgemerkt worden dat processoren nog steeds opstarten in real mode. Het is de taak van het besturingssysteem (of beter de loader ervan) om de processor om te schakelen naar protected mode. Andere

voorbeelden van extra functionaliteit zijn de integratie van functies die eerst door externe componenten werden vervuld. Bijvoorbeeld werd vanaf de 486 een floating point unit in de processor geïntegreerd. Een ander voorbeeld zijn cache geheugens. De extra functionaliteit uit zich ook op het vlak van de instructieset. Zo zijn in de loop der tijden een aantal extra instructies toegevoegd om aan bepaalde behoeften te voldoen. Een belangrijk voorbeeld zijn de instructies die het gebruik van multimedia moeten ondersteunen (bijvoorbeeld MMX,SSE, 3DNow) en de ondersteuning voor virtualisatie (bijvoorbeeld intel VT-d, amdVi). Software die gebruik maakt van dit soort instructies, kan uiteraard niet uitgevoerd worden op processoren die deze instructies niet ondersteunen. Intel, de grootste producent van x86 processoren, hanteert voor de ontwikkeling een model dat het tick/tock-model genoemd wordt. Afwisselend worden nieuwe modellen uitgebracht met nieuwe funcitonaliteit (tock) en verbeterde technologie (tick). Dit wordt duidelijk in volgende intel roadmap.

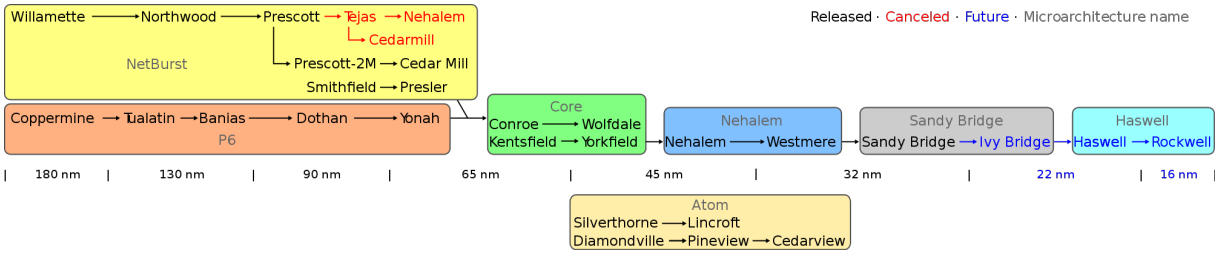

Figure 2.2. Intel roadmap (copyright 2008-2012 WhiteTimberwolf GFDL)

2.3. Kloksnelheid

Een tweede evolutie is waar te nemen op het vlak van de kloksnelheid, die duidelijk toegenomen is. In de beginjaren van de pc was te zien dat CPU klok en FSB klok samen toenamen. Na verloop van tijd ontstaat er een verschil tussen de processorklok en de FSB klok, die nog wel stijgt, maar een stuk minder snel. De processor wordt met andere woorden duidelijk het snelste onderdeel in het computersysteem. Het zal erop aan komen de werkkracht van de CPU zo weinig mogelijk onbenut te laten. In het bijzonder zullen maatregelen genomen moeten worden om zo weinig mogelijk tijd te verliezen bij het wachten op tragere componenten. De trend naar steeds stijgende kloksnelheden is tijdens het laatste decennium afgenomen. Bij de Pentium 4 werd nog volop gemikt op de 4GHz grens, waar enige jaren tegenaan gebotst werd. Belangrijkste probleem bij steeds hogere kloksnelheden is de gegenereerde warmte. Die moet in de eerste plaats uiteraard afgevoerd worden, maar geeft daarnaast ook nog een hoger verbruik.

In het bijzonder bij laptops zijn dit twee vervelende problemen: de warmteafvoer vraagt grotere (en dus zwaardere) koellichamen en ventilatoren. Extra verbruik verkleint uiteraard de autonomie van een draagbaar toestel (tijd dat op accu gewerkt kan worden).

2.4. Processorarchitectuur

2.4.1. Pipelining

Naast de kloksnelheid werd ook aan de interne opbouw van de processor gesleuteld om hem sneller bepaalde taken te laten uitvoeren. Zo werken processoren instructies niet na elkaar af, maar gedeeltelijk tegelijkertijd. Dit gebeurt in een zogenaamde pipeline. Het is eenvoudig om in te beelden dat terwijl de ene instructie uit het geheugen wordt opgehaald, een andere gedecodeerd kan worden en van nog een andere het resultaat berekend kan worden. Hieronder wordt dit principe grafisch voorgesteld. Helaas is dit principe niet zaligmakend: soms zijn instructies van andere, waardoor er een ‘bubble’ optreedt: een tijdspanne waarin de processor verplicht moet wachten.

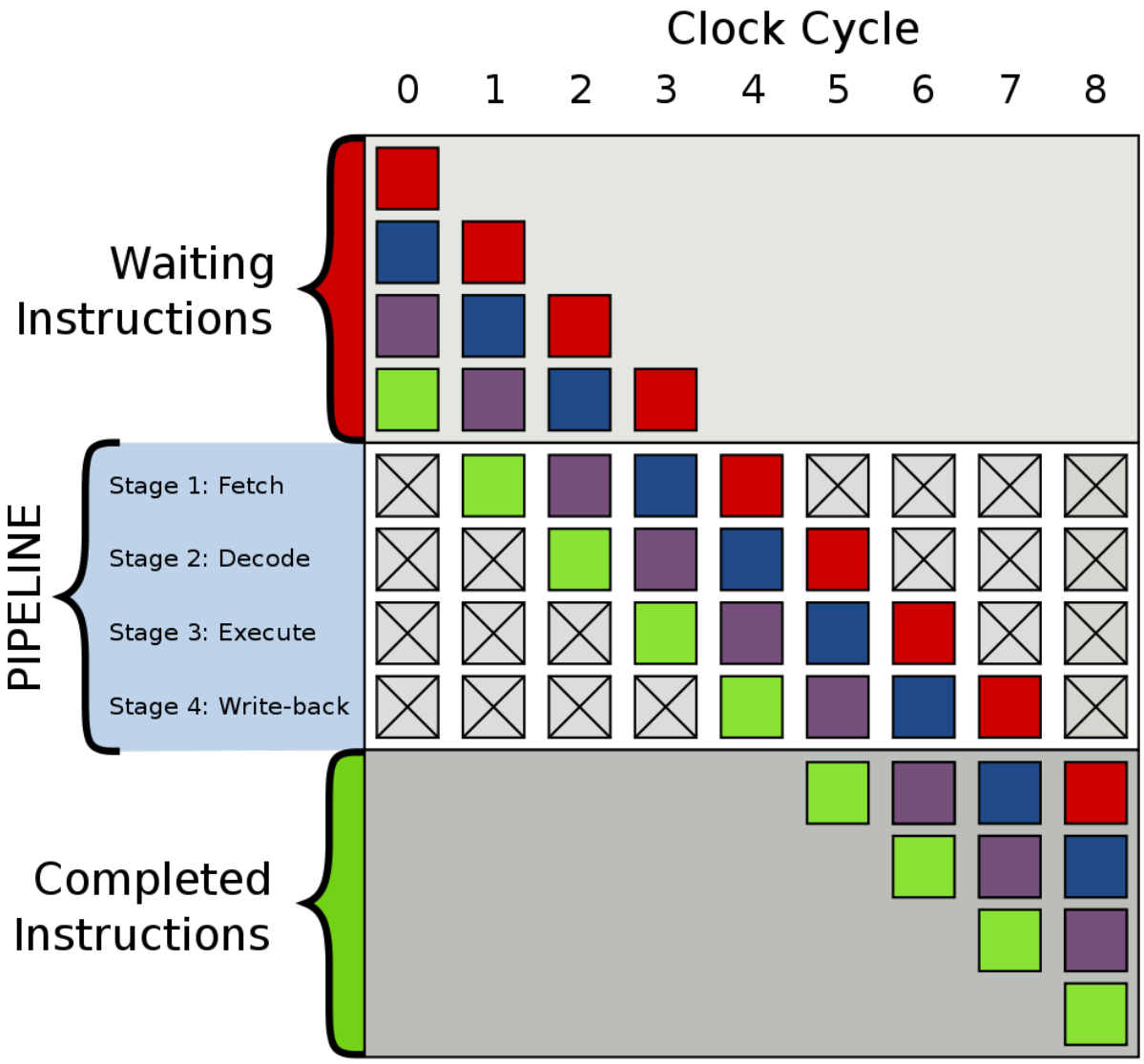

Figure 2.3. processor pipeline (CC mediawiki)

2.4.2. Superscalaire processoren

Als dit principe verder gedreven wordt, kunnen stappen die veel tijd in beslag nemen dubbel uitgevoerd worden. Men spreekt dan over een superscalaire processor. In afbeelding 8 en afbeelding 9 worden de blokschema's getoond van de Ivy bridge en de Athlon Bulldozer. In deze blokschema's is duidelijk te zien hoe er verschilllende eenheden zijn die berekeningen kunnen maken, waardoor verschillende instructies tegelijkertijd uitgevoerd kunnen worden. Een belangrijke uitdaging hierbij vormen voorwaardelijke sprong instructies. Aangezien pas bij de uitvoering van de instructie geweten is of de sprong uitgevoerd wordt of dat gewoon de volgende instructie wordt uitgevoerd. In het schema zijn hiervoor branch prediction eenheden voorzien. Meer details over hun werking en de

principes van pipelining en superscalaire architecturen krijg je in PC Architectuur 2: "microprocessoren".

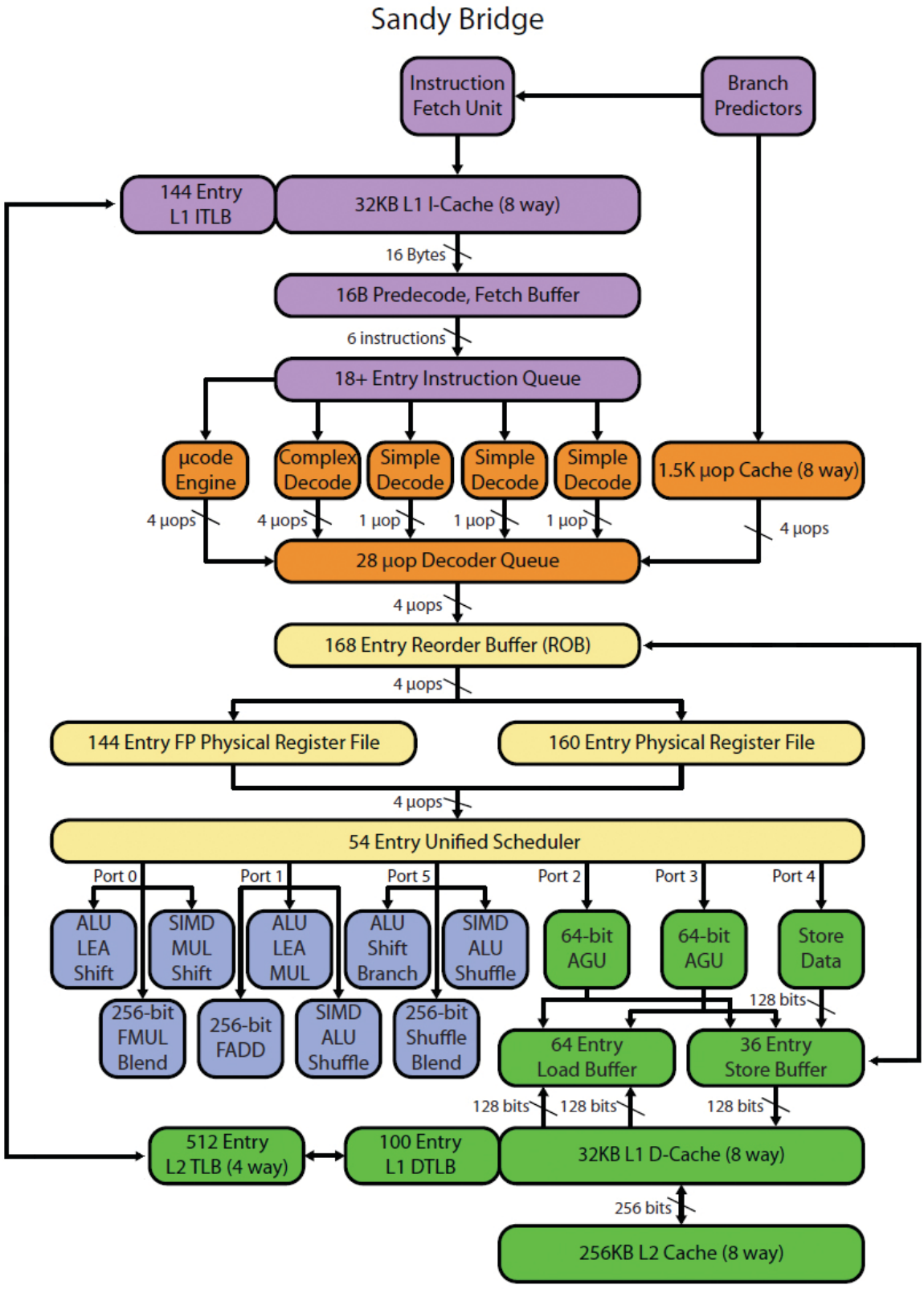

Figure 2.4. Sandy bridge microarchitectuur

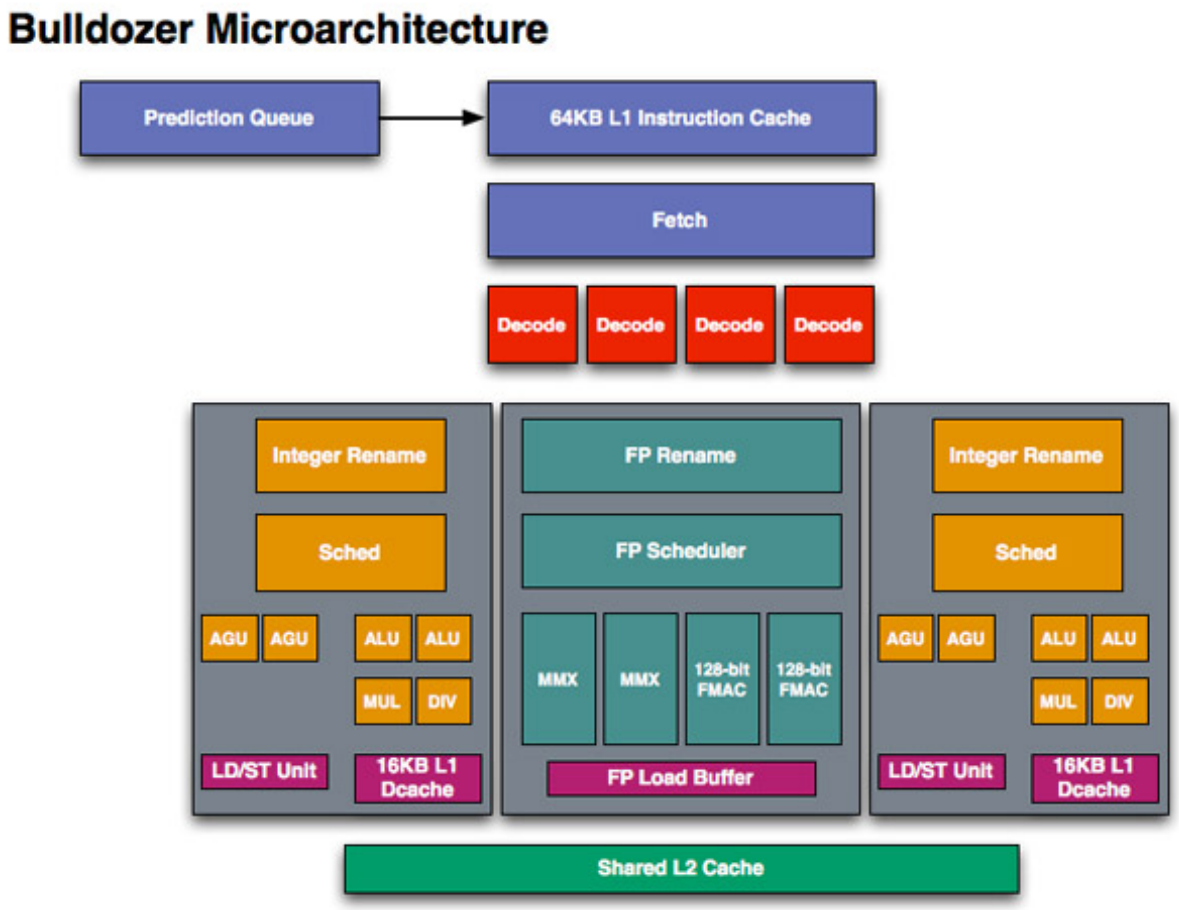

Figure 2.5. AMD bulldozer architectuur (copyright AnandTech)

Multicore processoren zijn al geruime tijd niet meer weg te denken. Hexacores en octocores zullen de komende jaren eerder regel dan uitzondering worden. Je zou dit een verder doorgedreven vorm van een superscalaire architectuur kunnen noemen. In plaats van delen van de processor te ontdubbelen, wordt een volledige processor ontdubbeld. Een grote moeilijkheid bij deze werkwijzes is om de caches op elkaar af te stemmen. Een probleem dat duidelijker zal worden in het volgende hoofdstuk. Net zoals een superscalaire architectuur pas voordeel geeft als de verschillende eenheden tegelijk gebruikt worden, zal een dual core pas voordeel geven als meerdere cores tegelijk werk verrichten. Dit kan als er bijvoorbeeld verschillende programma's tegelijk actief zijn of als de software zodanig geschreven is, dat ze bestaat uit verschillende threads die naast elkaar (en dus tegelijk door verschillende processorkernen) kunnen uitgevoerd worden. Een simpel voorbeeldje om de beperkingen van een multicore processor aan te tonen: als je een eenvoudige toepassing een rekenintensieve opdracht laat uitvoeren, dan zal een multicore processor slechts een deel belast worden. Eén processorkern verricht namelijk al het werk.

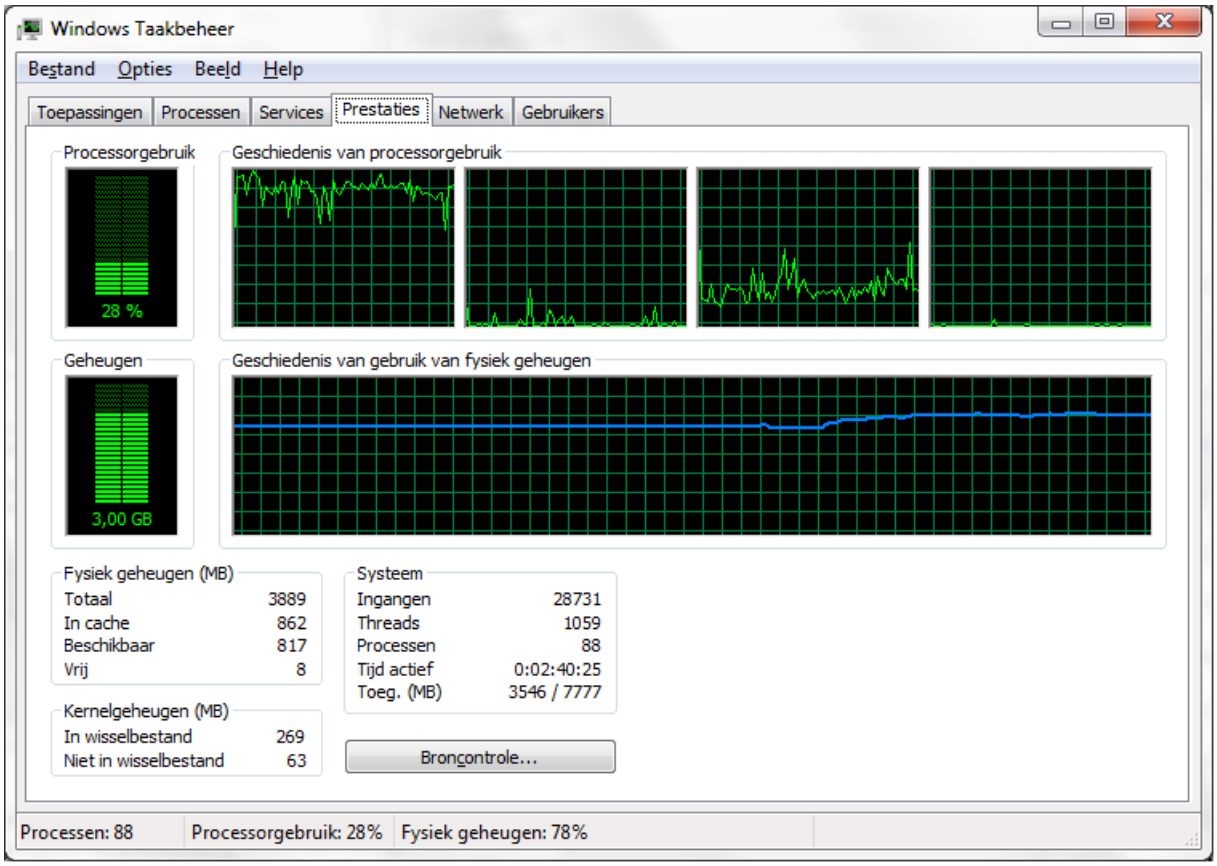

Figure 2.6. single threaded applicatie op multicore processor

Het voordeel van de multi-core merk je pas als je tegelijk nog een ander programma probeert te gebruiken. Dat zal met een multi-core vlot lukken, in tegenstelling tot een single core.

2.4.3. Cache

Een andere eigenschap die plots opduikt en doorheen de processorgeschiedenis steeds toeneemt is het cache geheugen. De toename van het cache volgt de trend van alle soorten geheugens die in een pc te vinden zijn. Dit is een gevolg van de eerder opgemerkte trend dat de processor veruit het snelste onderdeel is in het systeem, dat zo optimaal mogelijk benut moet worden. Naarmate data en programma's steeds groter werden, werd ook het belang van geheugen groter. Tot de intrede van de grafische interface was de belangrijkste parameter in het systeem de kloksnelheid van de processor. Met de intrede van de grafische interface was een groter geheugen soms te verkiezen boven een hogere kloksnelheid. Het belang van cache geheugen is ook duidelijk als je de budget- en performance-processoren van fabrikanten met elkaar gaat vergelijken.

In onderstaand lijstje staan enkele desktop en serverprocessoren opgelijst. Je merkt dat ze qua kloksnelheid niet voor elkaar moeten onderdoen, maar dat de hoeveelheden cache wel verschillen. Zo heeft bijvoorbeeld een high-end desktop CPU (core i7) zo'n 8MB cache aan boord, terwijl een serverCPU (Xeon E7) tot 32 MB cache heeft. De werking van de cache wordt verder in detail besproken in het derde hoofdstuk.

2.5. APU, SoC

De wet van Moore impliceert dat steeds meer mogelijk is op eenzelfde oppervlakte substraat. Die ruimte wordt ingenomen door bijvoorbeeld meerdere cores te huisvesten op eenzelfde processor, maar dat is maar een deel van het verhaal.

Het is namelijk ook zo dat men probeert om steeds meer functionaliteit te verzamelen op eenzelfde chip.

Daar zijn een aantal goede redenen voor te bedenken:

- het aantal verschillende chips op een moederbord kan zo teruggedrongen worden
- als alle componenten dicht bij elkaar zitten, zijn geen *trage* bussen nodig tussen deze onderdelen
- de oppervlakte die nodig is om het systeem te bouwen verkleint zo, een belangrijk argument bij de ontwikkeling van mobile devices.

Bij recente processoren zit bijvoorbeeld steeds vaker een grafische chip ingebouwd. Dan spreekt men niet meer over CPU, maar over *APU (=advanced processing unit)* om dit verschil in de verf te zetten.

Het integratieproces gaat soms zo ver dat je kan spreken van een *System On A Chip*: alle belangrijke onderdelen (cpu, gpu, IO) zitten dan verzameld op één enkele chip. De rol van secundaire chips ("de chipset") wordt dus steeds kleiner.

Op welke SoC is jouw telefoon gebaseerd?

2.6. Montage

Bij de montage van een processor moet je enkele zaken in acht nemen.

- De processor moet compatibel zijn met het moederbord. Meestal kom je dit te weten door de socket van de processor te vergelijken met die van het moederbord.
- De processor plaatsen moet gebeuren zonder het uitoefenen van kracht: de processor valt normaalgezien in z'n socket (ZIF: zero insertion force), waarna je hem kan inklemmen.
- Mobiele processoren zijn vaak vast op het moederbord gemonteerd, vervangen is dan onmogelijk.

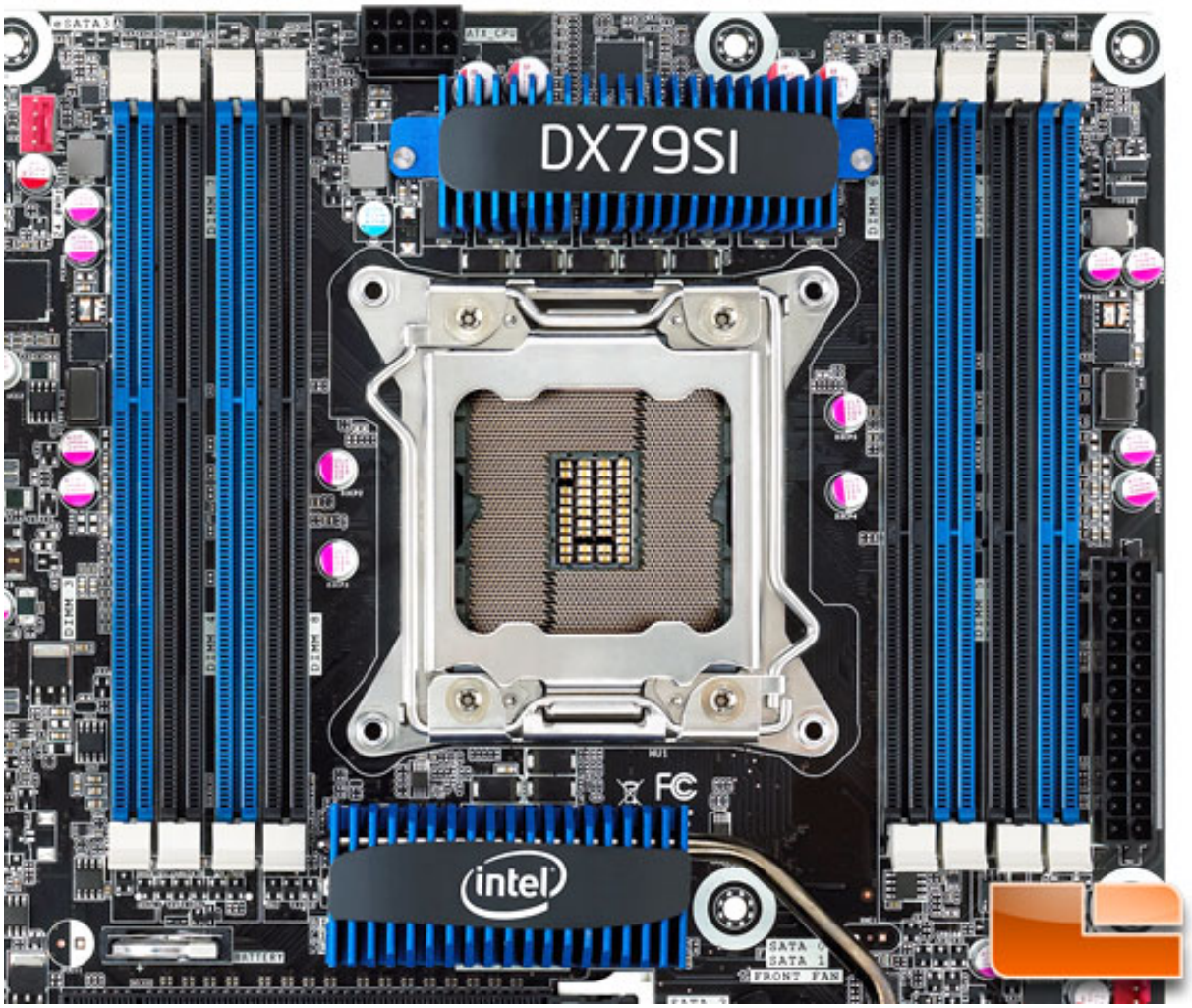

Figure 2.7. LGA2011 socket zonder processor

Tweede belangrijk aandachtspunt bij de installatie van een processor is dat gezorgd moet worden voor voldoende koeling. Dit betekent dat gezorgd moet worden voor een voldoende grote koelvin en ventilator en dat er goed contact is tussen de chip en de koelvin. Hiervoor moet eventueel koelpasta aangebracht worden. Een slecht gekoelde processor kan aanleiding geven tot een instabiel

werkende computer en in het meest dramatische geval tot een beschadigde processor.

2.7. Processoren van de toekomst

Voorspellingen maken is geen sinecure. De trends die ingezet zijn, zullen vermoedelijk nog een hele poos verder gaan, met een verdere miniaturisatie en toename van efficiëntie tot gevolg. Een kaper op de kust voor de x86 technologie is de ARM architectuur. Hoewel deze absoluut niet nieuw is (eerste ontwerpen midden jaren 80), biedt deze processorfamilie grote voordelen:

- Deze architectuur is steeds ontworpen voor toestellen met een laag verbruik. Het succes op de mobiele markt (iPAD2,3, nagenoeg alle android smartphones, consumer elektronica, ...)
- Deze architectuur is in licentie bij de meeste chipbakkers
- Door een RISC (Reduced instruction set computing) architectuur van nature efficient

De kans dat de RISC architectuur op korte termijn succesvol wordt op de desktopmarkt is gering, en ook het omgekeerde kan gezegd worden over CISC (x86) op mobiele devices. Voor specifieke servertoepassingen zijn er wel aankondigingen gebeurd[1] door bijvoorbeeld AMD, die zich hier sterk wil in specialiseren.

Toch lijken deze twee werelden van gespecialiseerde ARM en meer universele x86 naar elkaar toe te groeien, en zullen de grenzen ongetwijfeld snel vervagen. Microsoft heeft bijvoorbeeld eind 2012 z'n RT tablet vrijgegeven, met ARM SOC. Uiteraard zal software die gecompileerd werd voor x86 op dit soort toestellen niet werken.

2.8. Bibliografie bij dit hoofdstuk

[INTEL] Intel. http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html.

[1] http://www.anandtech.com/show/7724/it-begins-amd-announces-its-first-arm-based-server-soc-64bit8core-opteron-a1100

Chapter 3. Algemene bibliografie

[STALLINGS] Andy Hunt & Dave Thomas. *Computer Organization and architecture, Ninth edition*. Pearson education. 2012.

[RAMA] Umakishura Ramachandran. *Computer Systems: An Integrated Approach to Architecture and Operating Systems*. Manning Publications. 2010.