3. Cache-Subsysteme

3.1. Aufbau und Wirkungsweise des Cache-Subsystems

Caches sind zwischen Prozessor und Arbeitsspeicher angeordnet. Im folgenden geht es um Cache-Subsysteme außerhalb des Prozessorschaltkreises, also um *externe* Caches. Hat der Prozessor keine internen Caches, so ist die externe Schnellspeicheranordnung ein Cache der ersten Stufe (Level 1- bzw. L1-Cache). Beispiel: Systeme mit 386-Prozessor und externem Cache. Neuere Hochleistungsprozessoren (486, Pentium und andere) haben interne Caches. In solchen Konfigurationen ist die externe Schnellspeicheranordnung ein Cache der zweiten Stufe (Level 2- bzw. L2-Cache). Moderne Systeme wird man praktisch nicht mehr mit externen *L1*-Caches bauen: wenn, z. B. für bestimmte Embedded-Systems-Anwendungen, eine vergleichsweise geringe Prozessorleistung ausreicht, wird man beispielsweise einen 386 ohne externen Cache einsetzen. Genügt dessen Leistungsvermögen nicht, so ist der Übergang auf einen 486-Typ zweckmäßiger als die Erweiterung des 386 durch einen zusätzlichen Cache.

3.1.1. Realisierungsmöglichkeiten von L2-Caches

Ein moderner L2-Cache (Abbildung 3.1) besteht aus folgenden Funktionseinheiten:

- dem Datenspeicher (Daten-RAM),
- dem Kennzeichnungsspeicher (TAG-RAM),
- der Cache-Steuerung (Cache Controller).

Abbildung 3.44 Struktur eines L2-Caches

Hinweis:
Es handelt sich um eine Übersichtsdarstellung. Weitere Einzelheiten zeigen wir anhand ausgewählter Beispiele in Abschnitt 3.2.

Es gibt vielfältige Möglichkeiten, diese Funktionseinheiten auf Schaltkreise aufzuteilen (Tabelle 3.1), mit bestimmten Schaltkreistypen zu realisieren und die Schaltkreise z. B. auf Motherboards oder steckbaren Moduln anzuordnen (Tabelle 3.2).

Cache-Steuerung	TAG-RAM	Daten-RAM
■ spezielle Cache-Controller-Schaltkreise, ■ Funktionseinheiten in Motherboard-Steuer-schaltkreisen (Chip Sets), ■ mit programmierbarer Logik[1)]	■ übliche SRAMs, ■ spezielle TAG-RAMs, ■ im Controllerschaltkreis	■ übliche SRAMs, ■ synchrone SRAMs (Burst- oder Pipelined-Burst-SRAMs), ■ im Controllerschaltkreis

1): im PC-Bereich weniger üblich (ggf. nur in recht alter (386/486-) Hardware). Gelegentlich sind programmierbare Schaltkreise (PLDs, GALs) notwendig, um einen hochintegrierten Controller an die jeweilige Umgebung anzupassen (Rest- bzw. Glue-Logik).

Tabelle 3.1 Realisierungsmöglichkeiten der Funktionseinheiten externer Caches

Bei der Gestaltung des Cache-Subsystems können verschiedene Entwicklungsziele Vorrang haben:

- höchste Schaltungsintegration/höchste Geschwindigkeit,
- minimale Kosten,
- Erweiterbarkeit (Modularität).

Demzufolge finden wir eine Vielzahl von Ausführungen vor. Tabelle 3.2 gibt einen Überblick über Auslegungen externer Caches üblicher Personalcomputer.

Prozessor-Generation	Realisierung des externen Caches	Organisations-prinzipien	Länge eines Cache-Eintrags	Speicher-kapazität*)
386	Controller mit eingebautem TAG-RAM, Datenspeicher mit üblichen (asynchronen) SRAMs	wahlweise direktabbildend oder 2-fach block-assoziativ, Write Thru	1 Cache Line = 4 Bytes (32 Bits), 1 Block = 8 oder 16 aufeinanderfolgende Cache Lines (32 oder 64 Bytes)	32 oder 64 kBytes
486	TAG-RAM im Controller bzw. mit asynchronen SRAMs, Datenspeicher mit üblichen SRAMs	direktabbildend oder 2-fach block-assoziativ, Write Thru oder Write Back	1 Cache Line = 16 Bytes (128 Bits)	64 oder 128 kBytes
Pentium	TAG-Speicher mit üblichen SRAMs oder speziellen TAG-RAMs, Datenspeicher mit üblichen (asynchronen) oder mit synchronen (Pipelined Burst) SRAMs	direktabbildend, Write Back	1 Cache Line = 32 Bytes (256 Bits)	128, 256 oder 512 kBytes
Pentium Pro	gesamter L2-Cache auf einem Schaltkreis in gemeinsamem Gehäuse mit dem Prozessor	4-fach block-assoziativ, mehrere wählbare Schreib-verfahren (u. a. Write Back)	1 Cache Line = 32 Bytes (256 Bits)	256 oder 512 kBytes oder 1 MBytes
Pentium II**)	L2 Cache auf Prozessormodul, unabhängiger Cache-Bus (Dual Independent Bus Architecture)	wie Pentium Pro	wie Pentium Pro	wie Pentium Pro

*): typische Werte; **): siehe folgenden Hinweis 4

Tabelle 3.2 Typische Auslegungsformen externer Caches

Hinweise:

1. Tabelle 3.2 erfaßt keineswegs alle Varianten, die jemals verwirklicht worden sind. So gibt es bereits in PCs mit 386-Prozessoren eine beachtliche Zahl verschiedener Controller- und Speicherschaltkreistypen in vielfältigen Kombinationen und funktionellen Abwandlungen (z. B. auch 4-fach blockassoziative und

Write-Back-Caches).

2. Im Abschnitt 3.2. werden wir einige Ausführungsbeispiele kurz vorstellen.
3. Beruhend auf dem Prinzip der steckbaren Kassette (Single Edge Cartrige S.E.C.) werden verschiedene, nach Preis und Leistungsvermögen abgestufte Prozessor-Cache-Konfigurationen angeboten (auch: besonders preiswerte Typen *ohne* L2-Cache (Celeron)).
4. Womit weiterhin zu rechnen ist: L2-Caches auf dem Prozessorschaltkreis.

3.1.2. Technische Gestaltung kostengünstiger und modularer Cache-Subsysteme

Der Kostendruck des Marktes zwingt gleichsam den Entwickler dazu, bestimmte Auslegungen zu bevorzugen. Typische Anforderungen sind u. a.:

- Kostenminimierung: es sind vorwiegend Speicherschaltkreise aus der Massenfertigung einzusetzen,
- Möglichkeit der Produktdifferenzierung: Motherboards sind so zu gestalten, daß man auf Grundlage eines einzigen Typs mehrere - nach Leistungsvermögen und Kosten abgestufte Modelle fertigen kann (durch selektive Bestückung),
- Modularität (Baukastenprinzip): der Anwender soll seine Konfiguration nach Bedarf erweitern können.

Die gewählten Lösungen hängen vom jeweiligen Stand der Technik ab und sind dementsprechend dem Wandel unterworfen (Tabelle 3.3).

Herkömmliche PCs (386, 486, ältere Pentium-Modelle)	Moderne PCs des Massen-Marktes (Pentium und Kompatible)	Hochleistungssysteme
■ Controller mit eingebautem TAG-RAM, Fassungen für Daten-RAMs, ■ Controller mit eingebautem TAG-RAM, auf dem Motherboard Freiflächen bzw. Fassungen für Erweiterung des TAG-RAM sowie für die Daten-RAMs (selektive Bestückung), ■ TAG- und Daten-RAMs als asynchrone SRAMs auf Fassungen (Abbildung 3.2).	■ steckbare Speichermoduln mit TAG- und (vorzugsweise synchronen) Daten-RAMs (Abbildung 3.3a, b), ■ "Vollausbau" des Motherboards für das direkte Einlöten von TAG- und Daten-RAMs (bei preisgünstigeren Modellen selektiv bestückt; Abbildung 3.3c, d), ■ synchrone Daten-RAMs + Controller mit eingebautem TAG-RAM, ■ Grundausstattung der Datenspeicherkapazität in Controllerschaltkreisen, ggf. durch zusätzliche Daten-RAMs ergänzt, ■ L2-Cache auf Prozessorschaltkreis*)	■ komplettes Cache-Subsystem auf einem Schaltkreis, entweder mit dem Prozessor in einem gemeinsamen Gehäuse (z. B. Pentium Pro) oder auf steckbarem Modul (z. B. Pentium II), ■ Verbindung von Prozessor und L2-Cache über ein besonderes Bussystem (z. B. Dual Independent Bus Architecture DIB (Intel))

*): dies ist z. B. eine Möglichkeit, hochleistungsfähige, aber preisgünstige Prozessoren mit dem herkömmlichen Anschlußbild "Sockel 7" anzubieten

Tabelle 3.3 Auslegungs-Varianten von Speichersubsystemen

Abbildung 3.45 Cache-Konfigurationen mit asynchronen SRAMs

Erklärung:
Die Abbildung zeigt typische Bestückungsvarianten von 486-Motherboards (32-Bit-Datenbus). In Abbildung 3.2a, c sind die Datenspeicher in 2 Banks organisiert, die entweder im Interleaving oder im Sinne der Speichererweiterung (Näheres in Abschnitt 3.3.) betrieben werden. Die Bestückung gemäß Abbildung 3.2c kommt auch (bei anderer Schaltungsauslegung) für Pentium-Systeme in Frage (64-Bit-Datenbus).

Abbildung 3.46 Cache-Konfigurationen mit synchronen SRAMs (Quelle: Micron)

Erklärung:

a) Grundausstattung fest eingebaut (z. B. 256 kBytes; 2 PBSRAMs 32k · 32 + TAG-RAM 32k · 8 (asynchron)); Erweiterung durch ein steckbares Cache-Modul (Näheres in Abschnitt 3.4.),

b) der Cache ist ausschließlich als steckbares Modul vorgesehen (besonders preisgünstige Modelle werden ohne externen Cache ausgeliefert),

c) gesamte Cache-Ausstattung auf Motherboard, Möglichkeit der selektiven Bestückung (bei preisgünstigen Modellen entfallen die mit * gekennzeichneten Schaltkreise). Speicherkapazitäten z. B. 256/512 kBytes (mit Schaltkreisen 32k · 32) oder 512 kBytes/1 MBytes (mit Schaltkreisen 64k · 32).

d) gesamte Cache-Ausstattung auf Motherboard. Produkt-Differenzierung durch Bestückung mit entsprechenden RAMs (gemäß JEDEC-Standard; vgl. Kapitel 2, Abschnitt 2.3.). So lassen sich z. B. Speicherkapazitäten von 256 kBytes (mit Schaltkreisen 32k · 32) oder 512 kBytes (mit Schaltkreisen 64k · 32) realisieren.

Die Abbildung zeigt die Ausstattung typischer Pentium-Motherboards mit synchronen SRAMs (PBSRAMs) als Daten- und vorzugsweise asynchronen SRAMs als TAG-Speicher. Die Varianten a) und b) erlauben eine Cache-Erweiterung durch den Anwender; bei den Varianten b) und c) ist dies hingegen nicht möglich. (Auch professionelle Service-Werkstätten dürften kaum die Ausrüstung haben, TQFP-Gehäuse fachmännisch einzulöten. *Praxistip:* Nicht mit unzulänglicher Ausrüstung improvisieren - es dürfte sich nicht rechnen (von privaten Bastelübungen abgesehen).)

3.1.3. Cache-Verwaltung

Die Cache-Verwaltung muß gewährleisten, daß Einrichtungen (z. B. der Prozessor oder ein Bus-Master), die über den Cache auf den Speicheradreßraum zugreifen, im Cache immer gültige Daten vorfinden. Im folgenden geben wir einen Überblick über die hierzu notwendigen funktionellen Anforderungen. Diese betreffen:

1. das Abbildungsverfahren (Cache Organization),
2. das Schreibverfahren (Write Policy),
3. das Umgehen des Cache (Cache Policy),
4. das Einlagerungsverfahren (Allocation Policy),
5. das Auslagerungsverfahren (Replacement Policy),
6. die Kennzeichnung der Gültigkeit von Cache-Einträgen (Validity),
7. die Cache-Kohärenz (Cache Coherency),
8. das Abbildungsvermögen (Cacheability).

Hinweis:
In einem System mit mehreren Caches (externen und internen) muß die Cache-Verwaltung *alle* vorhandenen Caches berücksichtigen (so daß aus Sicht der Software wirklich die erforderliche “Transparenz” gewährleistet ist).

3.1.3.1. Abbildungsverfahren (Cache Organization)

Es sind die Verfahren “Direktabbildung “ (Direct Mapping) und “2- oder 4-fach blockassoziative Abbildung” (2 or 4 Way Set Associative Mapping) üblich.

Im Fach-Englisch steht “1 Way” für einen Adreßumsetzungsweg aus TAG-RAM und Adreßvergleicher (die Direktabbildung entspricht somit einem “1 Way Set Associaticve Mapping”). Je mehr Adreßumsetzungswege (man spricht dann auch von “höherer Assoziativität”), um so besser die Trefferrate des Cache, um, so höher aber auch der Aufwand. Es folgen einige grundlegende Zusammenhänge:

- Direktabbildung im Verbund mit dem Schreibverfahren Write-Thru ist die einfachste Lösung; sie kann mit asynchronen SRAMs als TAG-RAMs kostengünstig implementiert werden,
- Verfahren mit mehr als einem Adreßumsetzungsweg kann man nur mit speziellen Lösungen für die TAG-RAMs auf wirtschaftliche Weise verwirklichen (mit speziellen TAG-RAM-Schaltkreisen oder durch Einbau der TAG-RAM-Anordnung in den Controllerschaltkreis,
- kleine Caches (mit beispielsweise 32...128 kBytes) erreichen bei Direktabbildung nur unbefriedigende Trefferraten (deshalb hatte man seinerzeit für 386- und 486-Caches eine wenigstens 2-fach blockassoziative Auslegung bevorzugt; vgl. Abschnitt 3.2.1.),
- will man mit einem n-fach blockassoziativer Cache kürzeste Zugriffszeiten erreichen, so muß auch der Datenspeicher aus n parallel angeordneten Moduln aufgebaut werden. Es werden n Cache-Einträge (= 1 Block) parallel adressiert (und der Modul, dessen Adreßumsetzungsweg einen “Treffer” (Hit) signalisiert hat, wird ausgewählt). Dem gegenüber stehen kostenoptimierte Lösungen mit nur einer Datenspeicheranordnung. Hierbei sind die Cache-Einträge aller Adreßumsetzungswege in Behältern auf unterschiedlichen Adressen (z. B. aufeinanderfolgend) gespeichert (Pseudo n-Way Organization). Im Falle eines Treffers muß dann zunächst der Behälter des jeweiligen Adreßumsetzungsweges ausgewählt werden (Zeitverlust). Vgl. hierzu die Pseudo 2-Way Organization im Beispiel gemäß Abschnitt 3.2.8.
- bei vorgegebener Speicherkapazität des Datenspeichers hat ein direktabbildender Cache das größtmögliche Abbildungsvermögen (Cacheability; siehe Abschnitt 3.1.3.8.). Das Abbildungsvermögen (im Sinne von “x MBytes cacheable address space”) sinkt bei 2-fach blockassoziativer Organisation auf die Hälfte, bei 4-fach blockassoziativer Organisation auf 1/4.
- sind die Daten-RAMs vergleichsweise kostengünstig, so liegt es nahe, einen größeren direktabbildenden Cache vorzusehen (befriedigende Trefferraten auf Grundlage einfacher Steuerschaltkreise und preiswerter TAG-RAMs (meistens: herkömmliche asynchrone SRAMs); dies ist die typische Auslegung vieler PCs mit Pentium-Prozessor; vgl. weiter unten Abschnitt 3.2.3.),
- im oberen Leistungsbereich hat es hingegen keinen Sinn, den Cache bis in’s Extrem zu vergrößern (Stichwort: kapazitive Belastung der Signale durch die Schaltkreisanschlüsse - diese Tatsache gilt auch dann, wenn man die RAMs geschenkt bekäme)*),
- der Leistungsgewinn infolge des Cache-Subsystems ist stets eine statistische Angelegenheit (wer es darauf anlegt, kann für jede Cache-Lösung Programme schreiben, die nachweisen, daß die Prozessorleistung schlechter ist als ohne jeden Cache). Leistungsmessungen mit typischen Anwendungsprogrammen haben aber gezeigt, daß bei Cache-Größen zwischen 256 kBytes und ca. 1 MByte eine 2-fach blockassoziative Auslegung dieselbe Verbesserung der Trefferrate bewirkt wie die Verdoppelung eines direktabbildenden Cache. Deshalb bevorzugt man für Hochleistungssysteme wiederum blockassoziative Auslegungen.
- beim aktuellen Stand der Technik ist die 2-fach blockassoziative Organisation ein sinnvoller Kompromiß zwischen Aufwand, Trefferrate und Abbildungsvermögen.

*): der Ausweg: man ordnet eine weitere Cache-Ebene zwischen L2-Cache und Arebitsspeicher an (L3-Cache).

3.1.3.2. Schreibverfahren (Write Policy)

Es sind die Schreibverfahren “Write Thru” und “Write Back” üblich (Tabelle 3.4).

Schreibverfahren	Kennzeichen	Vorteile	Nachteile
Write Thru	jeder Schreibzugriff ist stets auch ein Arbeitsspeicherzugriff (auch bei einem Cache Hit)	keine DIRTY-Bits erforderlich, Schreibzugriffe wirken sich unmittelbar im Arbeitsspeicher aus [2)]	geringere Systemleistung
Write Back	Schreibzugriffe, die "Treffer" (Cache Hits) sind, betreffen zunächst nur den Cache[1)]	geringere Busbelastung, höhere Systemleistung	DIRTY-Bits im TAG-RAM erforderlich, kompliziertere Steuerung

1): zum Zurückschreiben s. folgenden Hinweis 4; 2): das ist manchmal funktionell notwendig (z. B. beim Schreiben in Bildspeicher)

Tabelle 3.4 Schreibverfahren

Hinweise:

1. Aus Leistungsgründen bevorzugt man in modernen Cache-Subsystemen das Write-Back-Verfahren.
2. Write-Back-Caches müssen im laufenden Betrieb von Zugriff zu Zugriff auf Write Thru umschaltbar sein, um den Architektur-Vorgaben der Prozessoren zu entsprechen (vgl. die PWT (Page Write Thru)-Bits in den Seitentabelleneinträgen).
3. Write Back erfordert je Cache-Eintrag ein Kennzeichnungsbit im TAG-RAM (DIRTY bzw. MODIFIED).
4. Zurückschreiben bei Write Back: das Zurückschreiben von Cache-Einträgen wird bei folgenden Anlässen ausgelöst:

    - der betreffende Cache-Eintrag soll durch einen neuen ersetzt werden (Cache Line Replacement),
    - durch Abläufe, die die Cache-Kohärenz gewährleisten,
    - durch entsprechende Maschinenbefehle zum Leeren des Caches (IA-32-Prozessoren: WBINVD = Write Back and Invalidate).

3.1.3.3. Umgehen des Cache (Cache Policy)

In den meisten Systemen dürfen Zugriffe auf bestimmte Teile des Speicheradreßraumes nicht über den Cache geführt werden, mit anderen Worten: sie sind vom "Caching" auszuschließen (Non-Cacheable Regions). Das betrifft z. B. Bildspeicher von Videoadaptern und andere E-A-Einrichtungen, die über den Speicheradreßraum angesprochen werden. Manchmal ist nur ein zeitweiliges Ausschließen erforderlich, beispielsweise um den Inhalt eines BIOS-ROM in den Arbeitsspeicher zu überführen (BIOS Shadowing).

Bei jedem Zugriff auf den Speicheradreßraum muß bekannt sein, ob der Cache umgangen werden soll oder nicht. Des weiteren ist (wenn der Cache hierfür die Wahl läßt) bei Schreibzugriffen das Schreibverfahren zu bestimmen. Hierfür gibt es verschiedene Möglichkeiten:

Softwareseitige Steuerung über entsprechende Architektur-Vorkehrungen im Prozessor

- die 486- und Pentium-Prozessoren haben Bitpositionen in Steuerregistern, über die man die Caches "global" steuern kann (CD = Cache Disable (Cache(s) außer Betrieb)),
- im Protected-Modus der .IA-32-Architektur (vom 386 an) kann man die Seitenverwaltung (Paging) ausnutzen. Die Seitenverzeichnis- und Seitentabelleneinträge enthalten hierfür die Bits PCD und PWT (PCD = Page Cache Disable, PWT = Page Write Thru). Darüber kann man den Speicheradreßraum seitenweise vom Caching allgemein ausschließen bzw. bestimmen, daß Schreibzugriffe auf bestimmte Seiten stets den Arbeitsspeicher mitbetreffen.
- Bereichsregister (Beispiel: Pentium Pro, Pentium II). Diese Prozessoren haben eine Anzahl spezieller Register, mit denen die Speicherkonfiguration gesteuert werden kann (Memory Type Range Registers; MTRRs). Diese Register enthalten Typfelder, in denen zu jedem Speicherbereich die zugehörige Betriebsweise des Cache-Subsystems angegeben wird.

Steuerung über die Hardware

Die Prozessoren und Steuerschaltkreise haben Steuereingänge, über die der Cache außer Betrieb gesetzt werden kann (übliche Signalbezeichnungen: KEN ≙ Cache Enable, NCA ≙ Non Cacheable Access). Bei jedem Speicherzugriff wird der KEN-Eingang abgefragt. Ist er aktiv, so wird der Cache umgangen. Indem man den KEN-Eingang durch entsprechende Adreßvergleicher oder -decoder ansteuert, kann man beliebige Adreßbereiche vom Caching ausschließen. (Extremfall: Cache gar nicht verwenden = KEN ständig inaktiv halten.)

Softwareseitige Steuerung über die Steuerschaltkreise (Cache Controller)

Manche Controllerschaltkreise enthalten einige (z. B. 4) universell ausgelegte Bereichsregister, um "Non Cacheable Regions" zu bestimmen (z. B. durch Laden einer Adreß- und einer Längenangabe). Oftmals hat man aber die Beeinflussungsmöglichkeiten an die PC-typische Aufteilung des Speicheradreßraumes angepaßt (es sind feste Bereiche vorgesehen, denen man bestimmte Attribute zuordnen kann; vgl. Abschnitt 3.2.2.).

3.1.3.4. Einlagerungsverfahren (Allocation Policy)

Grundsätzlich sind nur Zugriffe auf Adressen zu berücksichtigen, die nicht vom Caching ausgeschlossen sind. Das Problem der Einlagerung (Allocation) ergibt sich stets, wenn ein Zugriff auf eine dem Caching unterworfene (cacheable) Adresse ein Cache Miss ist. Folgende Einlagerungsverfahren als Reaktion auf einen Cache Miss sind üblich:

a) beim Lesen
Es wird *stets* ein Cache-Eintrag aufgebaut (Allocation on Reads).

b) beim Schreiben
Hier gibt es 2 Alternativen:

1. es wird *kein* Cache Eintrag aufgebaut (No Allocation on Writes),
2. es wird *stets* ein Cache Eintrag aufgebaut (Allocation on Writes).

Hinweise:

1. Allocation on Writes hat folgende Vorteile: (1) bessere Trefferrate (es ist recht wahrscheinlich, daß auf benachbarte Adressen (die den gleichen Cache-Eintrag betreffen) zugegriffen wird, (2) Verringerung der Busbelastung.
2. Allocation on Writes verspricht nur im Verbund mit dem Schreibverfahren Write Back nennenswert mehr Leistung (nach dem Einlagern des Cache-Eintrags wird nur in den Cache geschrieben).
3. Intel bevorzugt für 486 und Pentium *No Allocation on Writes*. Beim Pentium Pro bzw. Pentium II ist hingegen ausschließlich *Allocation on Writes* vorgesehen.
4. Es gibt Steuerschaltkreise, die es ermöglichen, das Einlagerungsverfahren bei Schreibzugriffen pro-

grammseitig (über ein Steuerregister) auszuwählen.

3.1.3.5. Auslagerungsverfahren (Replacement Policy)

Das Auslagern "alter" Cache-Einträge (um in den Behältern Platz für neue zu schaffen) ist an sich nur ein Problem bei einem blockassoziativen Abbildungsverfahren (bei Direktabbildung gibt es jeweils nur einen Behälter im Cache - und der wird einfach mit dem neuen Eintrag überschrieben). Um den freizumachenden Behälter zu bestimmen, wird meistens ein näherungsweises LRU-Verfahren verwendet.

Hinweis:
Veränderte (modifizierte) Cache-Einträge (beim Write-Back-Cache) müssen in den Arbeitsspeicher zurückgeschrieben werden, ansonsten genügt ein "Ungültigmachen" (Invalidation) oder ein bloßes "Einfüllen" des neuen Cache-Eintrags.

3.1.3.6. Gültigkeit von Cache-Einträgen (Validity)

Zugriffe auf den Speicheradreßraum dürfen Cache-Einträge nur dann ansprechen, wenn diese "gültig" (valid) sind (d. h. wenn der Cache-Eintrag dem Inhalt des Arbeitsspeichers unter der jeweiligen Adresse entspricht). Es gibt zwei Möglichkeiten, die Gültigkeit zu kennzeichnen:

1. im TAG-RAM ist jedem Eintrag ein Gültigkeitsbit (VALID-Bit) zugewiesen,
2. es gibt keine VALID-Bits; statt dessen wird der Cache so initialisiert, daß anfänglich alle Einträge gültig sind (vgl. Abschnitt 3.2.2.).

3.1.3.7. Cache-Kohärenz (Cache Coherency)

Der Begriff bezeichnet folgendes Problem:

- es gibt im System mehrere Einrichtungen, die den Inhalt des Arbeitsspeichers verändern können (mehrere Prozessoren, aber auch DMA-Hardware und Einrichtungen, die, z. B. am ISA- oder am PCI-Bus, Busmaster werden können),
- der einzelne Prozessor "sieht" den Arbeitsspeicher aber nur über sein Cache-Subsystem,
- es ist notwendig, zu gewährleisten daß alle Einrichtungen bei Zugriff auf eine bestimmte Adresse dort gleichermaßen die aktuellen Daten vorfinden.

(Anders herum gesehen: gibt es in einem System nur einen einzigen Prozessor und ist dies die einzige Einrichtung, die den Speicherinhalt verändern kann, so gibt es kein Problem der Cache-Kohärenz.)

Die bevorzuge Lösung: Fremdzugriffsprüfung (Snooping). Jeder Cache beobachtet die über den Systembus laufenden Zugriffe. Handelt es sich (1) um den Zugriff einer anderen Einrichtung, betrifft dieser aber (2) einen gültigen Cache-Eintrag, so muß etwas getan werden. Hierzu stehen folgende Maßnahmen zur Wahl:

- der betroffene Eintrag wird als "ungültig" (invalid) gekennzeichnet (Cache Line Invalidation). Greift die jeweilige Einrichtung (z. B. ein Prozessor) erneut auf den entsprechenden Adreßbereich zu, so wird demzufolge der Eintrag neu aufgebaut (= aus dem Arbeitsspeicher geholt) und hat somit den aktuellen Inhalt. Invalidation-Abläufe bestehen im wesentlichen im Zurücksetzen des betreffende Gültigkeitsbits (im TAG-RAM).
- der betroffene Eintrag wird automatisch (vom Cache Controller) neu aufgebaut (d. h. aktualisiert; dieses etwas kompliziertere Verfahren ist notwendig, wenn man auf Gültigkeitsbits im TAG-RAM verzichtet hat).

Hinweise:

1. Kann man über mehrere Bussysteme auf den Speicheradreßraum zugreifen (z. B. über den Prozessorbus, DRAM-Bus, ISA-Bus, PCI-Bus usw.), so sind alle Bussysteme gleichzeitig zu überwachen (was auf üblichen Motherboards dadurch erleichtert wird, daß alle Bussysteme in den Steuerschaltkreisen zusammengeführt sind; vgl. Abbildungen 3.8 und 3.11).
2. Der Cache Controller muß alle Caches (externe und interne) gleichermaßen berücksichtigen (wobei es vorkommen kann, daß verschiedene Verfahren anzuwenden sind - z. B. erfordert in der Anordnung gemäß Abbildung 3.8 der interne Cache eines 486 einen Invalidation-Buszyklus und der externe Cache das Aktualisieren des betroffenen Eintrags).
3. Bei Write-Thru-Caches können nur fremde Schreibzugriffe die Kohärenz beeinträchtigen. Bei Write-Back-Caches ist hingegen damit zu rechnen, daß sich die aktuellen (= vom Prozessor veränderten) Daten im Cache befinden, nicht aber im Arbeitsspeicher. Somit müssen hier auch fremde Lesezugriffe berücksichtigt werden (zu den Spitzfindigkeiten siehe Tabelle 3.12).

3.1.3.8. Abbildungsvermögen (Cacheability)

Der Begriff ist mit einer Zahlenangabe verbunden, die besagt, wie groß der Ausschnitt aus dem Speicheradreßraum ist, den der Cache abbilden kann. Der Wert hängt von folgenden Gegebenheiten ab (Abbildung 3.4):

- der Länge des Cache-Eintrags (Cache Line),
- der Speicherkapazität des Cache (Cache Size),
- der Adreßbreite im TAG-RAM.

Abbildung 3.47 Zum Abbildungsvermögen. a) Beispiel einer herkömmlichen Adreßaufteilung (64 MBytes Cacheability), b) Beispiel einer Adreßaufteilung für 2 GBytes Cacheability

Erklärung:
Eine (Byte-) Adresse der Länge a (in Bits) beschreibt einen Adreßraum von 2^a Bytes. Anhand eines direktabbildenden Caches ist dargestellt, wie die Adreßbits ausgenutzt werden:

1) die niedrigstwertigen Adreßbits adressieren das einzelne Byte im Cache-Eintrag. Einem Adreßabschnitt von *al* Bits entspricht ein Cache-Eintrag von 2^{al} Bytes.
2) die folgenden Adreßbits adressieren den einzelnen Eintrag bzw. Block im Cache. Einem Adreßabschnitt von *cs* Bits entspricht ein Cache mit 2^{cs} Einträgen bzw. Blöcken. Jeder Eintrag bzw. Block erfordert einen Speicherplatz im TAG-RAM.
3) diese Adreßbits *tw* dienen zum Vergleichen mit dem Adreßfeld im TAG-RAM.

Wieviele Bytes der Cache abbilden kann, wird offensichtlich dadurch bestimmt, wieviele Adreßbits die Cache-Hardware auswerten kann. Das Abbildungsvermögen umfaßt den gesamten Adreßraum (2^a Bytes), wenn gilt:

$tw + cs + cl = a$.

Das Abbildungsvermögen eines gegebenen Caches ergibt sich als Zweierpotenz der Adreßbits, die tatsächlich ausgewertet werden:

Abbildungsvermögen (Cacheability; in Bytes) = $2^{tw+cs+cl}$.

Beispiel einer (herkömmlichen) Adreßaufteilung (Abbildung 3.4a):

- a = 32 Bits (die gängige 32-Bit-Byteadresse),
- cl = 5 Bits (1 Cache Line = 32 Bytes = 256 Bits = 4 Worte zu 64 Bits ≙ 1 Pentium-Burstzyklus),

- cs = 13 Bits (≙ 8k Einträgen bzw. Blöcken = 32k Worten zu 64 Bits ≙ Aufbau des Cache mit zwei 32k · 32 PBSRAMs (vgl. Abbildung 3.3 und Abschnitt 3.2.4.),
- tw = 8 Bits (≙ TAG-RAM 8k · 8 (ohne Gültigkeits- und andere Kennzeichnungsbits)).

Die Cache-Hardware nutzt also 8 + 13 + 5 = 26 Bits aus. Hiermit ergibt sich eine Cacheability von 2^{26} Bytes = 64 MBytes.

Maßnahmen zur Verbesserung des Abbildungsvermögens (Abbildung 3.4b):

1. Vergrößerung des Caches. Beispiel: Datenspeicher aus 4 32k · 32 oder 2 32k · 64 PBSRAMs (= Verdoppelung der Speicherkapazität = 16k Einträge); demgemäß muß der TAG-RAM 16k Adreßvergleichsangaben aufnehmen können. Dies belegt ein Adreßbit mehr und verdoppelt das Abbildungsvermögen (auf 128 MBytes).
2. breiteres Adreßfeld im TAG-RAM. Beispiel: 12 Bits. Dies belegt 4 Adreßbits mehr und bedeutet eine Verbesserung auf das 16-fache.

Beide Maßnahmen zusammen beziehen also 5 weitere Adreßbits in das “Caching” ein. Das ergibt eine Cacheability von 2^{31} Bytes = 2 GBytes.

Tabelle 3.5 gibt einen Überblick über das Abbildungsvermögen typischer L2-Cache-Konfigurationen (optimiert für Pentium-Prozessoren: Cache-Eintrag = 32 Bytes, Direktabbildung). Die Tabelle enthält den Zusammenhang zwischen Cache-Größe, Abbildungsvermögen und der Breite der Adreßfelder im TAG-RAM. *Beispiel:* Welche Cacheability hat ein Cache von 256 kBytes mit einem TAG-RAM, der 10 Bits breite Adreßfelder enthält? - In der Zeile “Cache-Größe 256k” suchen wir die Adreßfeld-Breite = 10 Bits auf und finden eine “Cacheable Memory Size” von 256 kBytes.

Hinweis:
Geht es um Systeme mit 16 Bytes breiten Cache-Einträgen (typisch für 486-Prozessoren), so ist Tabelle 3.5 weiterhin nutzbar, wenn man die Angaben der “Cacheable Memory Size” jeweils halbiert (die Tabelle reicht dann von 32 MBytes bis 2 GBytes).

Cache-Größe (Bytes)	Realisierungs-beispiel (PBSRAMs)	Cache-Einträge = Speicherplätze des TAG-RAM	Breite der Adreßfelder im TAG-RAM bei gefordertem Abbildungsvermögen (Cacheable Memory Size) von 64 M...4 GBytes (in Bits)					
			64 M	256 M	512 M	1 G	2 G	4 G
128 k	2 · 16k · 32	4 k	9	11	12	13	14	15
256 k	2 · 32k · 32	8 k	8	10	11	12	13	14
512 k	4 · 32k · 32	16 k	7	9	10	11	12	13
1 M	4 · 32k · 64	32 k	6	8	9	10	11	12

Tabelle 3.5 Das Abbildungsvermögen (Cacheability) in Abhängigkeit von Cache-Größe und Organisation des TAG-RAMs. Cache-Eintrag = 32 Bytes (256 Bits), Direktabbildung

Hinweise:

1. Die Breite des Cache-Eintrags (Cache Line Size) von 32 Bytes = 256 Bits ist genau auf die Burstzugriffe der Pentium-Prozessoren abgestimmt. Eine Vergrößerung wäre deshalb wenig sinnvoll (sie wäre möglich, würde aber die Steuerung noch weiter komplizieren).
2. Der Übergang auf blockassoziative Abbildung bringt in Hinsicht auf das Abbildungsvermögen gar nichts (im Gegenteil: bei gleicher Gesamt-Kapazität des Datenspeichers hat z. B. ein 2-fach blockassoziativer Cache nur die halbe Cacheability eines direktabbildenden).
3. Wenn (aus Kostengründen) eine bestimmte Breite des TAG-RAM vorgegeben ist (z. B. 8 Bits), gleichzeitig aber ein größtmögliches Abbildungsvermögen gefordert wird, so muß man auf VALID- und DIRTY-Bits verzichten (das heißt, die Prinzipien Direktabbildung + Write Thru wählen und einen höheren Steuerungsaufwand zur Gewährleistung der Cache-Kohärenz in Kauf nehmen).
4. Zur Systemoptimierung: im praktischen Betrieb muß das Abbildungsvermögen nicht größer sein als nötig (d. h. als die installierte Arbeitsspeicherkapazität). Unter Beachtung dieser Bedingung kann man ohne weiteres - falls die Hardware die Möglichkeit bietet (Jumper, Setup-Einstellungen o. ä.) - einen Cache auf blockassoziativen Betrieb umstellen.
5. Die Cache-Steuerung legt den vom Cache erfaßten Adreßbereich typischerweise an das “untere Ende” des Adreßraumes. (Bei einer Cacheability von 64 MBytes erstreckt sich der erfaßte (“cacheable”) Adreßraum also von Adresse 0 bis zur Adresse 2^{26}-1.)
6. Die internen (L1-) Caches der Intel-Prozessoren gewährleisten die Cacheability des gesamten linearen Adreßraumes (4 GBytes).
7. Zu den Zusammenhängen zwischen Cache-Größe, Cacheability, Auslegung des Arbeitsspeichers und Systemleistung siehe Kapitel 7.

3.2. Ausführungsbeispiele

3.2.1. 386-Cache-Subsystem mit Intel 82385

Der 82385 ist ein Cache-Controller mit eingebautem TAG-RAM (Abbildungen 3.5 bis 3.7).

Merkmale:

- Abbildungsverfahren: wahlweise (über Konfigurationseingang) direktabbildend oder 2-fach blockassoziativ,
- Schreibverfahren: Write-Thru, gepuffert,
- Datenspeicherkapazität: max. 32 kBytes,
- Aufbau des Datenspeichers: mit externen asynchronen SRAMs (z. B. mit 4 Schaltkreisen 8k · 8),
- Länge eines Cache-Eintrags (Cache Line Size): 32 Bits (4 Bytes),
- Länge eines Blocks: 8 Einträge = 32 Bytes,
- Abbildungsvermögen: 4 GBytes (= der gesamte Adreßraum),
- Umgehen des Cache: Bei jedem Zugriff wird ein Steuereingang NCA# (Non Cacheable Access) abgefragt. Ist dieser aktiviert, wird der Cache umgangen. Es ist externe Hardware notwendig, die Zugriffe auf zu umgehende (non-cacheable) Adreßbereiche erkennt und NCA# entsprechend ansteuert.
- Gewährleistung der Cache-Kohärenz: der Schaltkreis ist an den Adreßbus und an Steuersignale des Prozessors angeschlossen. Er kann somit alle Schreibzugriffe überwachen. Betrifft ein Schreibzugriff einen gültigen Cache-Eintrag, so wird dieser im TAG-RAM als ungültig (Invalid) gekennzeichnet.

Abbildung 3.48 Blockschaltbild mit 82385; für Direktabbildung konfiguriert (Intel)

Abbildung 3.49 Blockschaltbild mit 82385; für 2-fach blockassoziative Abbildung konfiguriert (Intel)

Abbildung 3.50 Organisation des 82385 bei 2-fach blockassoziativer Abbildung (Intel). *): siehe Erklärung

Erklärung:
Der TAG-Speicher im Schaltkreis (von Intel gelegentlich als Cache Directory bezeichnet) ist in 2 Moduln (Banks) mit jeweils 512 Einträgen ("Sets") aufgeteilt. Jeder Eintrag betrifft einen Block aus 8 Cache Lines. Für jeden Block werden eine 18-Bit-Vergleichsadresse, ein zugehöriges Gültigkeitsbit (Tag Valid) sowie 8 weitere Gültigkeitsbits (Line Valid; ein Bit je Cache Line) gespeichert. Weiterhin ist je "Set" 1 LRU-Bit vorgesehen.

*): Die Adreßaufteilung zeigt, daß tatsächlich der gesamte 4-GBytes-Adreßraum erfaßt wird (18 Bits: Adreßvergleich, 9 Bits: Block-Auswahl im TAG-Speicher, 3 Bits: Auswahl des Cache-Eintrags im Block, 2 Bits (in der Abbildung nicht dargestellt): Auswahl des Bytes im Cache-Eintrag; 18 + 9 + 3 + 2 = 32 Bits).

3.2.2. 486-Cache-Subsystem mit Intel 82425EX

Der Schaltkreissatz 82420EX dient zum Aufbau von PCs mit 486-Prozessor, ISA-Bus und PCI-Bus (Abbildungen 3.8, 3.9). Die Cache-Steuerung ist Teil des Schaltkreises 82425EX (PSC = PCI System Controller).

Merkmale:

- Abbildungsverfahren: direktabbildend,
- Schreibverfahren: Write-Thru oder Write-Back,
- Datenspeicherkapazität: 64, 128, 256 oder 512 kBytes (auch: kein L2-Cache),
- Struktur der TAG-Einträge: 8 Bits Vergleichsadresse, 1 DIRTY-Bit (für Write Back). *Keine* VALID-Bits.
- Realisierung des TAG-Speichers: extern mit asynchronen SRAMs (siehe Tabelle 3.6),
- Aufbau des Datenspeichers: mit externen asynchronen SRAMs (z. B. mit 4 Schaltkreisen 32k · 8),
- Datenspeicher-Moduln (Banks): 1 oder 2, je nach Kapazität (vgl. Tabelle 3.6),
- Interleaving-Betrieb: möglich (Abbildung 3.9),
- Länge eines Cache-Eintrags (Cache Line Size): 16 Bytes (= 4 32-Bit-Worte ≙ 1 486-Burstzyklus),
- Abbildungsvermögen: siehe Tabelle 3.6,
- Umgehen des Cache: über Konfigurationsregister steuerbar (PAM-Register; Tabellen 3.8 bis 3.10),
- Gewährleistung der Cache-Kohärenz: der Schaltkreis hat Verbindungen zu allen in Betracht kommenden Bussystemen (Prozessorbus (Host-Bus), Arbeitsspeicher, PCI-Bus, ISA-Bus; vgl. Abbildung 3.8). Er kann somit alle Zugriffe überwachen (wesentlich sind hier DMA- und Busmaster-Zugriffe). Betrifft ein solcher Schreibzugriff einen Cache-Eintrag, so wird dieser automatisch aktualisiert (entsprechende Einträge im L1-Cache werden ungültig gemacht). Im Write-Back-Betrieb sind auch fremde Lesezugriffe zu berücksichtigen (einen Eindruck von den funktionellen Anforderungen vermittelt Tabelle 3.12 in Abschnitt 3.2.3.).
- Speisespannung: 5 V (Steuerschaltkreis + alle SRAMs).

Abbildung 3.51 Blockschaltbild eines Motherboards mit 82420EX-Schaltkreisen (Intel)

Abbildung 3.52 PSC-Schaltkreis 82425EX mit Cache aus 2 Moduln, die im Interleaving betrieben werden (Intel)

Erklärung:

1) Der Daten-RAM des Cache besteht aus insgesamt 8 asynchronen SRAMs 32k · 8 bzw. · 9. Zwei Banks aus je 4 SRAMs werden im Interleaving betrieben. Der “Intel-typische” Burst-Zyklus (4 32-Bit-Worte) bewirkt Zugriffe auf je 2 Worte in jeder Bank.
2) Der vollständige Cache-Eintrag wird über die SRAM-Adreßeingänge A14...A1 ausgewählt. Diese Adresse wird zu Beginn des Burst-Zyklus mit dem Gültigkeitssignal ADS bzw. EADS (Address Strobe) in ein Latch-Register übernommen. (ADS definiert die Zugriffs-Adresse des Prozessors, EADS die Adresse bei Fremdzugriffen (die zwecks Kohärenz-Prüfung - Snooping - sowohl dem internen Cache des Prozessors als auch dem L2-Cache zugeführt wird).) Umschaltung zwischen den Banks: über COE1#, COE0# (Output Enable; beim Lesen) bzw. CWE1#, CWE0# (Write Enable; beim Schreiben). Schaltkreisauswahl (CS#): beim Schreiben über die Byte-Enable-Signale (BE3...0), beim Lesen generell Wortauswahl: durch Ansteuern der SRAM-Adreßeingänge A0 (gesondert für jede Bank); CI3O2 für Bank 1 (Odd), CI3E für Bank 0 (Even). Die Steuersignale schalten so, daß sich die typische “interleaved”-Adreßfolge (Kapitel 2, Abbildung 2.6) ergibt.
3) Der TAG-RAM kann mit einem SRAM-Schaltkreis in · 9-Organisation aufgebaut werden (alternativ wäre die Realisierung mit je einem “· 8" und “· 1" organisierten Schaltkreis möglich; bei Beschränkung auf Write Thru könnte die 9. Bitposition entfallen).

Die Tabellen 3.6 bis 3.10 geben Einblick in weitere Einzelheiten.

Größe des Cache	SRAMs für Datenspeicher	Banks	TAG-SRAM	zum Adreßvergleich genutzte Adreßbits[1)]	Abbildungsvermögen (Cacheable Memory Size)
64 kBytes	8k · 8, 8 Stück	2	4k · 9	A23...16	16 MBytes
128 kBytes	32k · 8, 4 Stück	1	8k · 9	A24...17	32 MBytes
256 kBytes	32k · 8, 8 Stück	2	32k · 9	A25...18	64 MBytes
512 kBytes	128k · 8, 4 Stück	1	32k · 9	A26...19	128 MBytes

1): vgl. Abbildung 3.4

Tabelle 3.6 Cache-Konfigurationen

Art des Zugriffs	Interleaving	Zugriffszeit der Daten-SRAMs[1)]	Organisation des L1-Caches[2)]	Burstzugriffe des Prozessors (Taktzyklen)	
				bei 25 MHz	bei 33 MHz
Lesen	ja	15...20 ns	WT oder WB	2-1-1-1	2-1-1-1
	nein	15 ns	WT oder WB	2-1-1-1	2-2-2-2
	nein	20 ns	WT oder WB	2-1-1-1	2-2-2-2
Schreiben	ja	15...20 ns	WT oder WB	2-1-1-1[3)]	2-1-1-1[3)]
	nein	15...20 ns	WT	2-1-1-1[3)]	2-1-1-1[3)]
	nein	15...20 ns	WB	3-2-2-2	3-2-2-2

1): Zugriffszeit des TAG-RAMs: 15 ns; 2): WT = Write Thru, WB = Write Back,; 3): schnellster Zugriff bei Cache Hit

Tabelle 3.7 Zugriffszeiten

PAM-Register	Bits 7...4		Bits 3...0	
	Speicherbereich	Belegung	Speicherbereich	Belegung
0	F0000-FFFFH	BIOS		reserviert
1	C4000-C7FFFH	ISA-ROM	C0000-C3FFFH	ISA-ROM
2	CC000-CFFFFH	ISA-ROM	C8000-CBFFFH	ISA-ROM
3	D4000-D7FFFH	ISA-ROM	D0000-D3FFFH	ISA-ROM
4	DC000-DFFFH	ISA-ROM	D8000-DBFFFH	ISA-ROM
5	E4000-E7FFFH	BIOS-Erw.	E0000-E3FFFH	BIOS-Erw.
6	EC000-EFFFFH	BIOS-Erw.	E8000-EBFFFH	BIOS-Erw.

ISA-ROM = ROM-Erweiterungen auf ISA-Steckkarten; BIOS-Erw. = ROM-Bereiche für BIOS-Erweiterung.

Vgl. auch Fehlersuchhandbuch, Teil N, Abschnitt 2.14.

Tabelle 3.8 PAM-Register

Erklärung:
Im Schaltkreis sind 6 Konfigurationsregister (PAM6...0) vorgesehen (PAM = Progammable Attribute Map Register). Jedes PAM-Register ist 1 Byte breit, und jede Tetrade enthält 4 Attributbits, die dem jeweiligen Speicherbereich zugeordnet sind (Tabelle 3.9).

Attributbit	Wirkung, wenn Bit = 1	Wirkung, wenn Bit = 0
RE = Read Enable	Lesezugriffe des Prozessors betreffen den Arbeitsspeicher	Lesezugriffe des Prozessors betreffen den PCI- und in Folge den ISA-Bus[2)]
WE = Write Enable	Schreibzugriffe des Prozessors betreffen den Arbeitsspeicher	Schreibzugriffe des Prozessors betreffen den PCI- und in Folge den ISA-Bus[2)]
CE = Cache Enable[1)]	der Speicherbereich wird im Cache-Subsystem abgebildet	der Speicherbereich ist vom Caching ausgeschlossen
PE = PCI Enable	PCI-Busmaster können auf den Speicherbereich zugreifen	der Speicherbereich ist für PCI-Busmaster unzugänglich (diese können über den betreffenden Adreßbereich nur PCI- und in Folge ISA-Slaves erreichen[2)], nicht aber den Arbeitsspeicher)

1): zu den Spitzfindigkeiten in Zusammenhang mit CE = 1 sei auf das Intel-Datenmaterial verwiesen; 2): Zugriffe auf Adressen, die am PCI-Bus nicht belegt sind, werden automatisch zum ISA-Bus weitergeleitet

Tabelle 3.9 Die Attributbits der PAM-Register

Weitere Speicherbereiche haben eine implizite Attributzuordnung (Tabelle 3.10).

Adreßbereich	Belegung	Attribute
0H-9FFFH	Conventional Memory (DOS; 640 kBytes)	feste Zuordnung zum Arbeitsspeicher: Lesen, Schreiben, “cacheable”
A0000-BFFFFH	Video-Bildspeicher (128 kBytes)	feste Zuordnung zum PCI- und ISA-Bus, nicht “cacheable”
C0000-EFFFFH	BIOS-Erweiterungsbereiche (12 · 16 kBytes)	können über die PAM-Register 1...6 (Tabelle 3.8) konfiguriert werden
F0000-FFFFFH	BIOS (64 kBytes)	kann über PAM-Register 0 konfiguriert werden
100000-7FFFFFFH	Arbeitsspeicher (von 1M bis zur Obergrenze (128M))	feste Zuordnung zum Arbeitsspeicher: Lesen, Schreiben, “cacheable”
ab 8000000H	PCI-Adreßbereich, Flash BIOS	keine Arbeitsspeicherzugriffe, kein Caching

Tabelle 3.10 Implizite Speicheraufteilung im Schaltkreissatz 82420

Hinweise:

1. Nach dem Hardware-Rücksetzen greift der Prozessor auf das Flash-BIOS zu (1. Befehl von Adresse FF...F0H). Das Flash-BIOS belegt einen Adreßbereich von 512 kBytes. Dieser Bereich wird auf den Bereich der ISA-Bus-Adressen abgebildet (die entsprechenden Zugriffe werden auch zum ISA-Bus geführt), und zwar vom 16. MByte an abwärts (FFFFFF-F7FFFH).
2. Die Teile des Speicheradreßraumes, die dem Peripherie-Bussystem (PCI + ISA) zugeordnet sind, sind

grundsätzlich vom Caching ausgeschlossen.

Initialisierung des L2-Cache
Der TAG-RAM hat keine Gültigkeitsbits. Deshalb muß das BIOS den Cache anfänglich so initialisieren, daß es keine ungültigen Einträge gibt. Hierzu kann man den Cache programmtechnisch so umsteuern, daß er auf jeden Zugriff mit einem Cache Miss reagiert (Steuerbit "Force Miss Clean" im Cache-Steuerregister). Das BIOS schaltet zunächst dieses Bit ein und liest dann aus dem Arbeitsspeicher einen Bereich, dessen Länge der Größe des L2-Cache entspricht (der Bereich muß von einer entsprechenden integralen Adresse gelesen werden). Da jeder Zugriff zunächst ein Cache Miss ist, wird jeweils ein Cache-Eintrag aufgebaut, so daß am Ende dieses Ablaufs der gesamte Cache mit gültigen Einträgen (bei an sich beliebigem Inhalt) gefüllt ist.

3.2.3. Pentium-Cache-Subsystem mit Intel 82437FX

Der Schaltkreissatz 82430FX ("Triton-Chipset") dient zum Aufbau von PCs mit Pentium-Prozessor und PCI-Bus (Abbildungen 3.10 bis 3.13). Die Cache-Steuerung ist Teil des Schaltkreises 82437FX.

Merkmale:

- Abbildungsverfahren: direktabbildend,
- Schreibverfahren: Write-Back,
- Datenspeicherkapazität: 256 oder 512 kBytes (auch: kein L2-Cache),
- Struktur der TAG-Einträge: 8 Bits Vergleichsadresse, 1 VALID-Bit, 1 DIRTY-Bit,
- Realisierung des TAG-Speichers: extern mit asynchronem SRAM (Kennzeichnungsbits bei 256 kBytes vollständig, bei 512 kBytes teilweise im Steuerschaltkreis; siehe Tabelle 3.11),
- Aufbau des Datenspeichers: mit externen asynchronen oder synchronen Burst-SRAMs (Flow-Thru oder Pipelined; siehe Abbildungen 3.11 bis 3.13),
- Länge eines Cache-Eintrags (Cache Line Size): 32 Bytes (= 4 64-Bit-Worte ≙ 1 Pentium-Burstzyklus),
- Abbildungsvermögen: 64 MBytes (≙ der maximal anschließbaren Arbeitsspeicher-Ausstattung),
- Umgehen des Cache: über Konfigurationsregister steuerbar (PAM-Register; vgl. die Tabellen 3.8 bis 3.10 und die zugehörigen Erklärungen),
- Gewährleistung der Cache-Kohärenz: der Schaltkreis überwacht die Aktivitäten auf dem PCI-Bus und kann somit zweckmäßig reagieren, wenn PCI-Busmaster auf den Arbeitsspeicher zugreifen wollen (über den PIIX-Schaltkreis werden auch DMA- und ISA-Busmaster-Zugriffe erfaßt). Infolge der Write-Back-Organisation sind sowohl Lese- aus auch Schreibzugriffe zu berücksichtigen. Der Schaltkreis steuert die entsprechenden Prüfabläufe (Snooping) in beiden Caches (L1 und L2). Siehe dazu weiterhin Tabelle 3.12.
- Speisespannungen: 3,3 V und 5 V (5-V-TAG-SRAMs sind einsetzbar).

Abbildung 3.53 Blockschaltbild eines Motherboards mit 82430FX-Schaltkreisen (Intel)

Erklärung:
Der Schaltkreissatz umfaßt (als Bestückung eines Motherboards) folgende Schaltkreise:

- den System Controller (TSC) 82437FX,
- zwei Datenweg-Schaltkreise 82438FX (TDP; hiermit wird ein 64 Bits breiter Datenweg zwischen Prozessor/L2-Cache und Arbeitsspeicher verwirklicht, und zwar unter Zwischenschaltung von Lese- und Schreibpuffern),.
- einen Peripherie-Anschlußschaltkreis 82371FB (PIIX= PCI ISA IDE XCELERATOR); hiermit werden ein ISA-Bus und die übliche "Motherboard-Peripherie"dem PCI-Bus nachgeschaltet).

Cache-Größe	externer TAG-RAM	VALID-Bits	DIRTY-Bits	Inhalt des externen TAG-RAMs
256 kBytes	8k · 8	im Steuer-schaltkreis	im Steuer-schaltkreis	Vergleichsadresse (8 Bits)
512 kBytes	16k · 8	im externen TAG-SRAM	im Steuer-schaltkreis	Vergleichsadresse (7 Bits) + VALID-Bits (eines je Eintrag)

Tabelle 3.11 Realisierung des TAG-RAM

Fremdzugriff (von Busmaster)	Treffer (Snoop-Hit)		Reaktion
	im L1-Cache	im L2-Cache	
Lesen	nein	nein	-
	nein	ja[1)]	zurückschreiben und ungültig machen
	ja[1)]	nein	zurückschreiben
	ja[1)]	ja[1)]	aus dem L1-Cache zurückschreiben, im L2-Cache ungültig machen
Schreiben	nein	nein	-
	nein	ja	aus dem L2-Cache zurückschreiben[2)] und ungültig machen
	ja	nein	aus dem L1-Cache zurückschreiben[2)] und ungültig machen
	ja	ja	aus dem L1-Cache zurückschreiben[2)], in beiden Caches ungültig machen

1): beim Lesen sind nur Treffer auf modifizierte Einträge (enthalten geänderte Daten, DIRTY-Bit ist gesetzt) von Bedeutung; 2): ein Treffer auf einen modifizierten Eintrag führt zum Zurückschreiben, ein Treffer auf einen unmodifizierten Eintrag lediglich zum Ungültigmachen (VALID-Bit → 0)

Tabelle 3.12 Zur Wirkungsweise der Kohärenzprüfung (Snooping)

Erklärung:
Der Fremdzugriff betrifft stets den Arbeitsspeicher. Der eigentliche Arbeitsspeicherzugriff findet erst *nach* einem eventuellen Zurückschreiben statt. Es wird stets versucht, vor Ausführung des Fremdzugriffs im Arbeitsspeicher aktuelle Daten bereitzustellen. Hierzu werden modifizierte Cache-Einträge zurückgeschrieben. Das Zurückschreiben eines Cache-Eintrags bedeutet nichts anderes, als daß der entsprechende Speicherbereich (hier: von 32 Bytes Länge) im Arbeitsspeicher aktualisiert wird. Ein Lesezugriff findet somit stets aktuelle Daten vor, und beim Schreiben werden die aktellen Daten des Prozessors und des Busmasters gleichsam zusammengemischt. (Beispiel: der Prozessor hat das 3. und 4. Byte in dem betreffenden Speicherbereich verändert, und der Busmaster schreibt Daten in die 19. und 20. Byteposition desselben Bereichs.) Durch das Ungültigmachen des Cache-Eintrags wird gewährleistet, daß beim nächsten Zugriff des Prozessors wieder eine aktuelle Kopie des Speicherbereichs als neuer Cache-Eintrag herangeschafft wird.

Hinweis:
Daß sowohl Prozessor als auch Busmaster praktisch gleichzeitig auf dieselben Adressen schreiben, muß “auf

höherer Protokollebene" (z. B. mittels Systemsoftware) verhindert werden.

Die folgenden Abbildungen 3.11 bis 3.13 und Tabellen 3.12 bis 3.14 geben Einblick in weitere Einzelheiten.

Zu den Signalbezeichnungen in den Blockschaltbildern:
HA = Adresse des Prozessorbus (Host Address), HD = Daten des Prozessorbus (Host Data), HCLK = Prozessor-Bustakt (Host Clock).

Abbildung 3.54 256-kBytes-Cache mit asynchronen SRAMs

Erklärung:
Der Datenspeicher ist mit 8 SRAMs 32k · 8 aufgebaut. Diese erhalten ihre Adresse teils vom Prozessorbus, teils vom Steuerschaltkreis (die niedrigstwertigen Adreßsignale 1, 0 müssen vom Steuerschaltkreis geliefert werden, weil dieser die Burst-Adreßzählung ausführen muß). Da die Adresse vom Prozessorbus an 8 Schaltkreise zu liefern ist, sind Pufferstufen (P) zwischengeschaltet. Welche Zugriffszeiten die SRAMs haben müssen, ist in Tabelle 3.13 angegeben (die zugehörige Erklärung nennt auch die zulässigen Verzögerungszeiten der Pufferstufen).

Abbildung 3.55 256-kBytes-Cache mit synchronen (Flow-Thru-) Burst-SRAMs

Erklärung:
Es werden 4 Burst-SRAMs 32k · 16 verwendet (vgl. auch Kapitel 2, Abschnitt 2.2.2.). ADS# ist das Adreß-Strobe-Signal des Prozessors. Alternativ könnte ein solcher Cache auch mit 2 Schaltkreisen 32k · 32 oder mit einem Schaltkreis 32k · 64 aufgebaut werden.

Abbildung 3.56 512-kBytes-Cache mit synchronen Pipelined-Burst-RAMs (PBSRAMs)

Erklärung:
Es werden 4 Burst-SRAMs 32k · 32 verwendet (vgl. auch Kapitel 2, Abschnitt 2.2.3.). Diese werden als 2 Banks betrieben, allerdings nicht im Interleaving, sondern gleichsam hintereinandergeschaltet (Näheres dazu in Abschnitt 3.3.). Alternativ könnte ein solcher Cache auch mit 4 Schaltkreisen 64k · 16, mit 2 Schaltkreisen 64k · 32 oder mit einem Schaltkreis 32k · 64 aufgebaut werden. Es sind sowohl Flow-Thru- als auch Pipelined-Typen einsetzbar (wie der Steuerschaltkreis auf den installierten Speichertyp eingestellt werden kann, wird in Abschnitt 3.2.5. beschrieben). Aus Tabelle 3.13 sind die Anforderungen an die Zugriffszeit von Flow-Thru-Schaltkreisen ersichtlich. Pipelined-Schaltkreise müssen mindestens für die jeweilige Taktfrequenz (50, 60, 66 MHz) spezifiziert sein.

Datenspeicher-Bestückung	asynchrone SRAMs		synchrone (Flow Thru Burst) SRAMs	
Prozessor-Bustakt	Daten-RAMs	TAG-RAM	Daten-RAMs[4)]	TAG-RAM[5)]
50 MHz	20 ns[1)]	30 ns	13,5 ns	20 ns
60 MHz	17 ns[2)]	20 ns	10 ns	15 ns
66 MHz	15 ns[3)]	15 ns	8,5 ns	15 ns

1)...5) siehe Erklärung im Text

Tabelle 3.13 Anforderungen an die Speicherschaltkreise (Zugriffszeiten)

Erklärung:

1) Verzögerungszeit zwischengeschalteter Pufferstufen: max. 17 ns,
2) Verzögerungszeit zwischengeschalteter Pufferstufen: max. 10 ns,

3) Verzögerungszeit zwischengeschalteter Pufferstufen: max. 7 ns,
4) Kennwert: Zugriffszeit von Taktflanke bis zum Erscheinen der Daten (t_{CDV}: Data Output Valid after Clock Rise; vgl. Kapitel 2, Abschnitt 2.1.1.).
5) der TAG-RAM ist stets ein asynchroner SRAM.

Tabelle 3.14 veranschaulicht das Leistungsvermögen entsprechender L2-Caches anhand der Bustakte, die die verschiedenen Zugriffe des Prozessors erfordern.

Art des Zugriffs	Dauer des prozessorseitigen Zugriffs (Prozessor-Bustakte)	
	mit asynchronen RAMs	mit synchronen RAMs
wahlfreies Lesen (Single Read)	3	3
wahlfreies Schreiben (Single Write)	4	3
Lesen im Burstbetrieb	3-2-2-2	3-1-1-1
Zurückschreiben (Write Back L1 → L2) im Burstbetrieb	4-3-3-3	3-1-1-1
aufeinanderfolgende (Pipelined Back-to-Back) Lesezugriffe im Burstbetrieb	3-2-2-2-3-2-2-2	3-1-1-1-1-1-1-1

Tabelle 3.14 Zum Leistungsvermögen des L2-Caches

Hinweise:

1. Bei Einsatz synchroner Burst-SRAMs werden Burstzugriffe nur um einen Wartezustand verlängert (Taktschema ohne jeden Wartezustand: 2-1-1-1; vgl. Fehlersuchhandbuch, Teil N, Kapitel 5)..
2. Für den einzelnen Zugriff hat es keinen Einfluß, ob Flow-Thru- oder Pipelined-Schaltkreise verwendet werden. Pipelined-Typen ermöglichen es aber, aufeinanderfolgende Lese-Burstzugriffe (Back-to-Back-Zugriffe) ohne Wartezustände aneinanderzureihen (zum Sonderproblem des Übergangs von einer Datenspeicher-Bank zur anderen siehe Abschnitt 3.3.).

3.2.4. Pentium-Cache-Subsystem mit Intel 82439HX

Der Schaltkreissatz 82430HX dient zum Aufbau von PCs mit Pentium-Prozessor und PCI-Bus (Abbildungen 3.14, 3.15). Die Cache-Steuerung ist Teil des Schaltkreises 82439HX. Der 82430HX gehört zur gleichen Familie wie der zuvor beschriebene Schaltkreissatz 82430FX; er enthält Verbesserungen, weicht aber in seinen Funktionen nicht grundsätzlich von den Vorgängertypen ab.

Merkmale:

- Abbildungsverfahren: direktabbildend,
- Schreibverfahren: Write-Back,
- Datenspeicherkapazität: 256 oder 512 kBytes (auch: kein L2-Cache),
- Struktur der TAG-Einträge: 8...11 Bits Vergleichsadresse, 1 VALID-Bit, 1 DIRTY-Bit,

- Realisierung des TAG-Speichers: extern mit asynchronem SRAM (Kennzeichnungsbits bei 256 kBytes vollständig, bei 512 kBytes teilweise im Steuerschaltkreis; siehe Tabelle 3.15),
- Aufbau des Datenspeichers: mit externen Pipelined-Burst-SRAMs (PBSRAMs; asynchrone oder Flow-Thru-RAMs sind *nicht* einsetzbar),
- Länge eines Cache-Eintrags (Cache Line Size): 32 Bytes (= 4 64-Bit-Worte ≙ 1 Pentium-Burstzyklus),
- Abbildungsvermögen: üblicherweise 64 MBytes, zusätzlich wählbar: 128, 256 oder 512 MBytes,
- Umgehen des Cache: über Konfigurationsregister steuerbar (PAM-Register; vgl. weiter oben die Tabellen 3.8 bis 3.10 und die zugehörigen Erklärungen),
- Gewährleistung der Cache-Kohärenz: vgl. die entsprechenden Erläuterungen zum 82437FX (Abschnitt 3.2.3.),
- Speisespannungen: 3,3 V und 5 V (5-V-TAG-SRAMs sind einsetzbar).
- Leistungsvermögen: vgl. Tabelle 3.14, rechte Spalte.

Abbildung 3.57 Blockschaltbild eines Motherboards mit 82430HX-Schaltkreisen (Intel)

Erklärung:
Der Schaltkreissatz umfaßt (als Bestückung eines Motherboards) folgende Schaltkreise:

- den System Controller (TSC) 82439HX (der Arbeitsspeicher ist über einen 72-Bit-Datenbus (ECC-Unterstützung) direkt an den System Controller angeschlossen; besondere Datenweg-Schaltkreise sind also nicht erforderlich),

- einen Peripherie-Anschlußschaltkreis 82371SB (PIIX3 = PCI ISA IDE XCELERATOR); hiermit werden dem PCI-Bus ein ISA-Bus, die übliche "Motherboard-Peripherie" sowie eine USB-Steuerung nachgeschaltet). (USB = Universal Serial Bus.)

Besonderheiten (1): erweitertes Abbildungsvermögen
Üblicherweise wird ein SRAM in · 8-Organisation als TAG-RAM angeschlossen. Hierfür sind die Datenanschlüsse TIO7...0 vorgesehen. Die Erweiterung des Abbildungsvermögens (siehe Tabelle 3.15 sowie Abschnitt 3.1.3.8.) erfordert einen "breiteren" TAG-RAM. Hierfür sind weitere Datenanschlüsse TIO10...8 vorgesehen, um maximal 11 Bits breite TAG-RAMs einsetzen zu können. *Implementierungsbeispiele:* (1) ein · 8-SRAM + ein · 4-SRAM, (2) zwei · 8-SRAMs, (3) ein · 16-SRAM. Die Erweiterung wird teils über das Cache-Steuerregister (siehe weiter unten Abschnitt 3.2.5.) und teils durch Außenbeschaltung gesteuert:

- Pull-down-Widerstand an TIO10: erweitertes Abbildungsvermögen (Extended Cacheability), sofern im Steuerregister aktiviert,
- Pull-up-Widerstand an TIO10: Unterstützung eines DRAM-Cache (vgl. Kapitel 2, Abschnitt 2.4.2.).

TIO9, 8 sind intern mit Pull-Down-Widerständen beschaltet (Festbelegung bei Nichtnutzung).

Zum Schaltkreissatz passende Cache-Moduln - vgl. Abschnitt 3.4. - haben je nach Bestückung eine entsprechende Widerstandsbeschaltung der Signale TIO10...8.

Besonderheiten (2): L2-Cache mit DRAM-Cacheschaltkreisen
Wird TIO10 fest mit High beschaltet (Pull-up-Widerstand), so ist die Unterstützung für DRAM-Caches aktiv (vgl.

Kapitel 2, Abschnitt 2.4.2., Tabelle 2.23 und Abbildung 2.34).

Die Funktionen “erweitertes Abbildungsvermögen” und “DRAM-Cache” schließen einander aus.

Cache-Größe	TAG-RAM	Abbildungsvermögen (Cacheability)
256 kBytes	8k · 8	64 MBytes
	8k · 9	128 MBytes
	8k · 10	256 MBytes
	8k · 11	512 MBytes
512 kBytes	16k · 8[1)]	64 MBytes
	16k · 9[1)]	128 MBytes
	16k · 10[1)]	256 MBytes
	16k · 11[1)]	512 MBytes

1): einschließlich dem VALID-Bit; vgl. auch Tabelle 3.11

Tabelle 3.15 Auslegung des TAG-RAM in Abhängigkeit von Cache-Größe und Abbildungsvermögen

Abbildung 3.58 256-kBytes-Cache mit Pipelined-Burst-SRAMs (zu den Anforderungen an die Speicherschaltkreise siehe Tabelle 3.16)

Prozessor-Bustakt	Zugriffszeit der PBSRAMs [1)]	Zugriffszeit des TAG-RAMs
50 MHz	13,5 ns	20 ns
60 MHz	10 ns	15 ns
66 MHz	8,5 ns	15 ns

1): die Speicher müssen mindestens für die jeweilige Taktfrequenz (50, 60, 66 MHz) spezifiziert sein; des weiteren ist die angegebene Zugriffszeit einzuhalten (t_{CO}: Data Output Valid after Clock Rise; vgl. Kapitel 2, Abschnitt 2.1.2.)

Tabelle 3.16 Anforderungen an die Speicherschaltkreise (Zugriffszeiten)

3.2.5. Cache-Konfiguration über Steuerregister

Die Cache-Konfiguration wird typischerweise über softwareseitig ladbare Register (Cache-Steuerregister) eingestellt. Als Beispiel zeigt Abbildung 3.16 die Belegung des Cache-Steuerregister der Intel-82430-Schaltkreissätze.

Abbildung 3.59 Das Cache-Steuerregister der Schaltkreissätze Intel 82430

Erklärung:

a) Registerbelegung. Die Felder bzw. Bits im einzelnen:

- SCS = Secondary Cache Size = installierte Speicherkapazität,
- SRAMT = SRAM Type,
- NAD = NA Disable. NA# (Next Address) ist ein Eingang der Pentium-Prozessoren, über den das Pipelining der Prozessor-Zugriffe gesteuert wird (das Aktivieren von NA# bewirkt, daß der Prozessor sofort den nächsten Zugriff startet, auch wenn ein aktueller Burstzugriff noch nicht beendet ist).
- ECE = Extended Cacheability Enable (bei manchen Schaltkreisen, z. B. beim 82347FX, reserviert). ECE = 0: Abbildungsvermögen auf 64 MBytes beschränkt; ECE = 1: Abbildungsvermögen auf 512 MBytes erweitert.
- SCFMI = Secondary Cache Force Miss or Invalidate. Steuert die Treffer-Erkennung im L2-Cache. SCFMI = 0: Normalbetrieb des L2-Caches (Treffer werden erkannt); SCFMI = 1: Treffer werden grundsätzlich nicht erkannt (jeder Zugriff ist ein Cache Miss). Anwendung: zum Testen und zum Initialisieren des L2-Caches.
- FLCE = First Level Cache Enable. Steuert die Nutzung des L1-Caches (im Prozessor). FLCE = 0: L1-Cache grundsätzlich außer Betrieb (Steuerschaltkreis hält KEN# inaktiv); FLCE = 0: L1-Cache zugeschaltet (Steuerschaltkreis aktiviert KEN#).
- Tabelle 3.17 zeigt, welche Wirkungen die Steuerbits SCMFI und FLCE zusammen ausüben.

b) Zuführung von Cache-Größe und Speichertyp beim Rücksetzen. Das gesamte Register kann softwareseitig geladen werden. Beim Rücksetzen werden aber die Bitpositionen 7...4 hardwareseitig eingestellt, indem die Belegung der Adreßeingänge 31...28 mit der Low-High-Flanke des /RESET-Signale übernommen wird. Dies ermöglicht es, die Cache-Konfiguration von außen einzustellen (z. B. mit Jumpern). Notwendig ist hierfür ein Treiber, der die Signale auf die Adreßeingänge (die während des Rücksetzens hochohmig sind) aufschaltet.

*): Alternativ zu den Jumpern können hier Erkennungssignale (Presence Detect; z. B. von Cache-Moduln) direkt oder über kombinatorische Netzwerke (die die jeweilige Presence-Detect-Belegung in Cache Konfigurationssignale umschlüsseln) angeschaltet werden. Vgl. auch Abschnitt 3.4.

FLCE		Wirkung
0	0	beide Caches vollständig außer Betrieb
0	1	Normalbetrieb beider Caches (Betrieb des L2-Caches hängt vom Feld SCS ab)
1	0	beide Caches außer Betrieb; Einträge im L2-Cache werden bei Lesezugriffen ungültig (d. h. die VALID-Bits werden gelöscht). Anwendung: z. B. zur Initialisierung der VALID-Bits.
1	1	beide Caches in Betrieb; alle Zugriffe (Lesen und Schreiben) auf den L2-Cache werden zu Cache Misses

Tabelle 3.17 Kombinierte Wirkung der Cache-Steuerbits SCFMI und FLCE

3.2.6. Pentium-Cache-Subsystem mit Cypress hyperCache-Schaltkreisen

Die hyperCache-Schaltkreissätze hC-ZX, hC-VX und hC-DX dienen zum Aufbau von PCs mit modernen Hochleistungsprozessoren (Pentium, AMD, Cyrix u. a.) und PCI-Bus (Abbildung 3.17; weitere Einzelheiten in den folgenden Abschnitten 3.2.7. und 3.2.8.) Die Cache-Steuerung ist Teil des Schaltkreises CY82C691.

Merkmale:

- Abbildungsverfahren: wahlweise direktabbildend oder 2-fach blockassoziativ,
- Schreibverfahren: wahlweise Write-Back oder Write-Thru,
- Datenspeicherkapazität: 128, 256, 384 (128 + 256) oder 512 kBytes,
- Struktur der TAG-Einträge: siehe weiter unten Abbildung 3.22,
- die TAG-Einträge haben *keine* VALID-Bits,
- Realisierung des TAG-Speichers: vollständig im Steuerschaltkreis,
- Aufbau des Datenspeichers: mit synchronen Burst-RAMs (Flow Thru oder Pipelined). Auch "gemischte" Bestückungen sind möglich. In die Datenwegschaltkreise ist eine "Grundausstattung" von 64 bzw. 128 kBytes eingebaut.
- Länge eines Cache-Eintrags (Cache Line Size): 32 Bytes (= 4 64-Bit-Worte ≙ 1 Pentium-Burstzyklus),
- Abbildungsvermögen: 128, 256 oder 512 MBytes,
- Umgehen des Cache: über spezielle PCI-Konfigurationsregister steuerbar (blockweise Steuerung ähnlich jener der oben beschriebenen Intel-Typen),
- Gewährleistung der Cache-Kohärenz: vgl. die entsprechenden Erläuterungen zum 82420EX (Abschnitt 3.2.2.),
- Speisespannungen: 3,3 V und 5 V,
- Leistungsvermögen: schnellstmögliche Burstzugriffe in 2-1-1-1 bzw. (mit Pipelined-Burst-RAMs) in 3-1-1-1 Takten; "langsamere" Betriebsweisen (z. B. 3-2-2-2 oder 4-2-2-2) sind einstellbar.

Abbildung 3.60 Blockschaltbild eines Motherboards mit hyperCache-Schaltkreisen (Cypress)

Erklärung:
Ein Schaltkreissatz umfaßt (als Bestückung eines Motherboards) folgende Schaltkreise:

- den System Controller CY82C691 mit eingebautem TAG-RAM für den L2-Cache,
- die DRAM-Datenwegschaltkreise CY82C190 (eingebauter L2-Cache: 64 kBytes) bzw. CY82C192 (eingebauter L2-Cache: 128 kBytes). Es ist jeweils nur ein Datenwegschaltkreis notwendig.
- die Peripheriesteuerung CY82C693 (Variante /U mit USB-Controller),
- (wahlweise) Cache-Erweiterungs-RAMs CY82C694 (siehe weiter unten Abbildung 3.24). Der L2-Cache kann aber auch mit "industrieüblichen" Burst-SRAMs erweitert werden.

Die Schaltkreise sind zum Aufbau preisgünstiger, aber trotzdem leistungsfähiger Motherboards vorgesehen und gestatten es, eine Vielzahl von Bestückungsvarianten (auch: mit Prozessoren verschiedener Hersteller) zu realisieren.

3.2.7. Zugriffsabläufe zum L2-Cache

Solche Abläufe sind selten dokumentiert. Wir nehmen hier das Cypress-Datenmaterial als Grundlage, um anhand einiger beispielhafter Abläufe die Nutzung der Pipelined-Burst-SRAMs (PBSRAMs) in L2-Caches näher zu erklären (Abbildungen 3.18 bis 3.21).

Abbildung 3.61 Prozessor-Lesezyklus (3-1-1-1-Burst) mit L2-Cache-Hit (Cypress). Der L2-Cache ist mit Pipelined-Burst-SRAMs bestückt

Erklärung:

1) der Prozessor zeigt den Beginn des Zugriffs durch Aktivieren von /ADS an,
2) mit /ADS wird die Adresse in den Datenspeicher übernommen (/ADS ist mit den /ADSP-Eingängen der

RAMs verbunden),

3) idealerweise müßten *vor* dieser Taktflanke die Daten bereitstehen, damit der Prozessor sie ohne Wartezustände übernehmen kann (2-1-1-1-Zyklus). Ein Pipelined-Speicher legt die Daten aber erst *nach* dieser Taktflanke auf den Datenbus. Deshalb wird ein Wartezustand eingelegt (/BRDY inaktiv; 3-1-1-1-Zyklus).
4) /ADVA (das /ADV-Signal der betreffenden Bank des L2-Cache) wird aktiv, damit im übernächsten Taktzyklus das nächste Wort gelesen werden kann (Adreßzählung),
5) die ersten Daten (D1) werden vom Prozessor übernommen. Um dem Prozessor die Gültigkeit der Daten anzuzeigen, ist vor der Taktflanke /BRDY aktiviert worden (kein Wartezustand mehr).
6) bei aktivem /ADVA wird in jedem Taktzyklus ein weiteres Datenwort übernommen (D2...D4). /BRDY wird dabei ständig aktiv gehalten.
7) aus Sicht des Prozessors ist mit der Übernahme des 4. Datenwortes (D4) der Burstzyklus beendet.

*) Aktivierung von /ADVA schadet nicht (Don't Care): Adresse zählt auf den Anfangswert zurück.

Abbildung 3.62 Prozessor-Lesezyklus (4-2-2-2-Burst) mit L2-Cache-Hit (Cypress)

Erklärung:
Diese Betriebsweise kann im Steuerschaltkreis programmseitig eingestellt werden (um preisgünstigere, aber langsamere Speicher einsetzen zu können). Es ist ersichtlich, daß der Ablauf gegenüber dem von Abbildung 3.18 nur durch Einfügen weiterer Wartezustände modifiziert wurde:

1)...3) siehe Erklärung zu Abbildung 3.18,
4) es wird ein zusätzlicher Wartezustand eingefügt (/BRDY bleibt weiter inaktiv). Deshalb darf auch die Adresse nicht weitergezählt werden (/ADVA ebenfalls inaktiv).
5) die ersten Daten (D1) werden vom Prozessor übernommen. Um dem Prozessor die Gültigkeit der Daten anzuzeigen, ist vor der Taktflanke /BRDY aktiviert worden. Des weiteren wurde /ADVA aktiviert, um eine Adreßzählung zu veranlassen.
6) vor der Taktflanke wird /BRDY wieder deaktiviert, um einen Wartezustand einzufügen. Entsprechend muß auch /ADVA deaktiviert werden (um ein nochmaliges Zählen zu verhindern). Daß das erste Datenwort (D1) weiterhin auf dem Datenbus liegt, ergibt sich aus der Wirkungsweise der RAMs (/ADSP = /ADSC = /ADV = High ≙ Wieder-Lesen des zuvor adressierten Wortes; vgl. Tabelle 2.16 in Kapitel 2, Abschnitt 2.2.3.8.) und hat ansonsten keine weitere Bedeutung.
7) es laufen noch 3 weitere solche Zugriffe (mit jeweils einem Wartezustand) ab.

Abbildung 3.63 Prozessor-Schreibzyklus (3-1-1-1-Burst) mit L2-Cache-Hit (Cypress)

Erklärung:

1) der Prozessor zeigt den Beginn des Zugriffs durch Aktivieren von /ADS an,
2) mit /ADS (= /ADSP) wird die Adresse in den Datenspeicher übernommen,
3) idealerweise könnten mit dieser Taktflanke die ersten Schreibdaten vom Prozessor übernommen werden (ADSP-gesteuertes "spätes" Schreiben; vgl. Abbildung 2.28 und Tabelle 2.17 in Kapitel 2, Abschnitt 2.2.3.8.). Die Hardware ist aber nicht so schnell. Deshalb wird ein Wartezustand eingelegt (/BRDY inaktiv).
4) das erste Datenwort vom Prozessor (D1) liegt nun an und kann mit der Taktflanke übernommen werden. Um dem Prozessor anzuzeigen, daß er das nächste Datenwort liefern darf, wird vor der Taktflanke /BRDY aktiviert.
5) Infolge des zuvor eingefügten Wartezustandes ist das ADSP-gesteuerte späte Schreiben (= Übernahme im folgenden Taktzyklus; hier handelt es sich aber um den *übernächsten*) nicht anwendbar. Deshalb aktiviert der Steuerschaltkreis /ADSC, um den Schreibvorgang zu starten (frühes Schreiben = Übernahme

mit der aktuellen Taktflanke; vgl. Abbildung 2.29 und Tabelle 2.18 in Kapitel 2, Abschnitt 2.2.3.8.).

6) /ADVA (das /ADV-Signal der betreffenden Bank des L2-Cache) wird aktiv, damit im nächsten Taktzyklus das nächste Wort geschrieben werden kann (Adreßzählung),

7) bei aktivem /ADVA wird in jedem Taktzyklus ein weiteres Datenwort in den L2-Cache geschrieben (D2...D4). /BRDY wird dabei ständig aktiv gehalten.

8) aus Sicht des Prozessors ist mit der Übernahme des 4. Datenwortes (D4) der Burstzyklus beendet,

*) Aktivierung von /ADVA schadet nicht (Don't Care): /ADVA ist wirkungslos, weil /ADSC aktiv ist (vgl. Tabelle 2.10 in Kapitel 2, Abschnitt 2.2.3.8.).

Abbildung 3.64 Prozessor-Lesezugriff mit L2-Cache-Miss auf einen modifizierten Eintrag (Cypress). Der L2-Cache ist mit Pipelined-Burst-SRAMs bestückt. Das untere Diagramm ist die Fortsetzung des oberen

Erklärung:

1) der Prozessor zeigt den Beginn des Zugriffs durch Aktivieren von /ADS an,

2) mit /ADS (= /ADSP) wird die Adresse in den Datenspeicher übernommen,

3) die Cache-Steuerung stellt fest, daß es sich um einen Cache Miss handelt. Zudem wird festgestellt, daß der Behälter im Cache von einem modifizierten Eintrag belegt ist (DIRTY-Bit gesetzt). Also muß dieser Eintrag zunächst in den Arbeitsspeicher transportiert werden. Anschließend ist ein neuer Cache-Eintrag aus dem Arbeitsspeicher heranzuschaffen.

4) dieses Rückschreiben wird hier mit *Castout* bezeichnet. Aus Sicht des L2-Caches sind Lesezugriffe auszuführen (die Schreibsteuersignale /CWE7...0 sind inaktiv). Nur werden die Daten nicht vom Prozessor abgenommen, sondern in den Arbeitsspeicher geschrieben.

5) das Schreiben ist Angelegenheit der DRAM-Steuerung. Im Beispiel hat der DRAM-Datenweg FIFO-Schreibpuffer, so daß in jedem Taktzyklus ein 64-Bit-Wort abgesetzt werden kann. /ADV wird deshalb ständig aktiv gehalten, und der Cache-Lesevorgang entspricht dem von Abbildung 3.18 (würde es länger dauern - z. B. in einer Hardware ohne FIFO-Schreibpuffer, so würde jeder Zugriff mehr als einen Taktzyklus benötigen, und /ADV müßte zwischendurch immer wieder inaktiv geschaltet werden (vgl. Abbildung 3.19)).

6) der neue Eintrag wird aus dem Arbeitsspeicher gelesen und in den L2-Cache geschrieben (*Fill Data*). Die Daten werden dabei gleichzeitig dem Prozessor angeboten.

7) das Lesen ist Angelegenheit der DRAM-Steuerung. Da hier nichts gepuffert ist, sind "richtige" DRAM-Zugriffe notwendig, die im Beispiel als Page-Mode-Zugriffe (mit ständig aktivem /RAS und schaltendem /CAS) ausgeführt werden. Die DRAM-Adresse wird dabei von der DRAM-Steuerung entsprechend weitergezählt (*Fill Address*). Jeder /CAS-Impuls entspricht einem DRAM-Zugriff mit der jeweiligen *Fill Address*, der ein 64-Bit-Wort (*Fill Data*) liefert. Wenn Page-Mode-Zugriffe nicht ausführbar sind, wären "volle" RAS-CAS-Zugriffe notwendig (die entsprechend mehr Takte erfordern). Während der DRAM-Zugriffe wird der Prozessor im Warten gehalten (/BRDY inaktiv). Ebenso werden die Schreibzugriffe zum Cache-RAM ausgesetzt (/ADSC = /ADV = /CWE7...0 =High ≙ Warten (Suspend Burst Write; vgl. Abbildung 2.29 und Tabelle 2.18 in Kapitel 2, Abschnitt 2.2.3.8.)).

8) um die vom Arbeitsspeicher kommenden Datenworte in den L2-Cache zu schreiben, wird ein frühes Schreiben durch Aktivieren von /ADSC gestartet. /ADV wird zunächst inaktiv.

9) bisher wurde der Prozessor durch /BRDY = Low im Wartezustand gehalten. Liegt das erste Datenwort auf dem Bus, so wird /BRDY für einen Taktzyklus aktiviert, damit der Prozessor ebenfalls (parallel zum L2-Cache) die Daten abnehmen kann.

10) es folgen noch 3 derartige Zugriffe, um den gesamten Cache-Eintrag heranzuschaffen. Bei jedem Zugriff werden die Schreiberlaubnissignale /CWE7...0 sowie /ADV aktiviert (Adreßzählung). *Achtung:* der erste dieser 3 Zugriffe ist einmal im oberen und einmal im unteren Diagramm dargestellt.

Hinweise:

1. Wie bei DRAMs, Bussystemen usw. setzen sich die vielfältigen Abläufe aus wenigen Grundfunktionen zusammen. Moderne Steuerschaltkreise enthalten unabhängige Steuerautomaten (State Machines) für die einzelnen Schnittstellen (zum Prozessor, zum L2-Cache, zum DRAM, zum PCI-Bus usw.). Infolge dessen ist bei den Abläufen mit einer Vielzahl von Kombinationen zu rechnen (die auch in den umfangreichsten Datenbüchern nicht darstellbar sind). Um sich einzuarbeiten, beginnt man am besten mit den Grundabläufen an den einzelnen Schnittstellen und versucht dann, das Zusammenwirken zu verstehen. *Praxistip:* mit dem jeweils "einfacheren" Bauelement anfangen - versuchen Sie also, zunächst den PBSRAM, den DRAM usw. zu verstehen, ehe Sie sich das Daten"blatt" eines Steuerschaltkreises vornehmen.
2. Lieferant der Adresse ist typischerweise entweder der Prozessor oder eine Busmaster- bzw. DMA-Hardware (z. B. ein PCI-Busmaster). (Mögliche Ausnahme: die Cache-Steuerung liefert die Adresse selbst, um den Cache zu leeren (Flush-Operation) bzw. um modifizierte Einträge in den Arbeitsspeicher zurückzuschreiben (z. B. im Sinne der Ausführung des Maschinenbefehls WBINVD = Write Back and Invalidate).)
3. Der Cache ist kein Dual-Port-RAM. Die Cache-Steuerung muß deshalb konkurrierende Zugriffe "serialisieren", also nacheinander ausführen.
4. *Zu den Adreß-Strobe-Eingängen der Cache-RAMs* (vgl. Kapitel 2, Abschnitt 2.2.3.):

   - ADSP: ist direkt mit dem ADS-Ausgang des Prozessors verbunden. Dieser kann somit jederzeit "seine" Adresse in den Cache bringen. Will die Cache-Steuerung dies verhindern, so muß sie entweder die Cache-RAMs deaktivieren (über die CE-Eingänge) oder den Prozessor im Wartezustand halten (beim vorhergehenden Zugriff, d. h. ehe er ADS aktivieren kann).
   - ADSC: wird von der Cache-Steuerung erregt. Mögliche Anlässe: (1) Starten von Schreibzugriffen mit der anliegenden Prozessor-Adresse (vgl. die Abbildungen 3.20, 3.21), (2) Zugriffe mit Fremdadressen (z. B. von einem Busmaster), (3) "eigene" Zugriffe.

3.2.8. Weitere Einzelheiten zu den hyperCache-Schaltkreisen

Die Abbildungen 3.22 und 3.23 sowie Tabelle 3.18 zeigen weitere Einzelheiten der hyperCache-Schaltkreise.

Abbildung 3.65 Struktur der TAG-Einträge im CY82C691

Erklärung:

- der TAG-RAM hat 8k Einträge zu 21 Bits (jeweils 2 10-Bit-Adreßvergleichsangaben + 1 gemeinsames LRU-Bit),
- die 10-Bit-Felder können folgendermaßen aufgeteilt sein:
  a) sie enthalten ausschließlich eine 10-Bit-Adreßangaben. Hiermit ergibt sich das maximale Abbildungsvermögen.
  b) sie enthalten eine 9-Bit-Adreßangabe und ein DIRTY-Bit (Write-Back-Betrieb). Dies halbiert praktisch das Abbildungsvermögen.
- VALID-Bits gibt es nicht; also muß die Cache-Steuerung dafür sorgen (mit entsprechender Initialisierung durch das BIOS), daß der Cache stets gültige Einträge enthält (vgl. weiter oben (Abschnitt 3.2.3.) den Schaltkreis Intel 82420FX).
- auch ohne DIRTY-Bits ist ein Write-Back-Betrieb möglich. Die Steuerung nimmt dann an, daß alle Einträge stets DIRTY (modifiziert) sind (Leistungsminderung durch gelegentlich unnötiges Rückschreiben).
- Betriebsweisen:

- direktabbildend,
- 2-fach blockassoziativ mit 2 Datenspeicher-Banks,
- 2-fach blockassoziativ mit 1 Datenspeicher-Bank (“Pseudo 2 Way”-Modus; dies kann zum Einfügen weiterer Wartezustände führen, so daß z. B. anstelle von 3-1-1-1-Zyklen 5-1-1-1-Zyklen ausgeführt werden).

Cache-Größe	1 Bank		2 Banks	
	ohne DIRTY-Bit	mit DIRTY-Bit	ohne DIRTY-Bit	mit DIRTY-Bit
128 kBytes	128 MBytes	64 MBytes	128 MBytes	64 MBytes
256 kBytes	256 MBytes	128 MBytes	256 MBytes	128 MBytes
384 kBytes	-	-	256 MBytes	128 MBytes
512 kBytes	512 MBytes	256 MBytes	256 MBytes	-

Tabelle 3.18 Das Abbildungsvermögen der verschiedenen Daten- und TAG-RAM-Konfigurationen

Abbildung 3.66 Der Erweiterungs-RAM CY82C694 (Cypress). Oben: Blockschaltbild, unten: Anschlußbelegung (TQFP, 168-polig)

Erklärung:
Der Schaltkreis ist ein synchroner Pipelined-Burst-SRAM der Organisationsform 16k · 64 (≙ 128 kBytes). Die Abbildung veranschaulicht - als Beispiel der “Industriestandard”-Auslegung - sowohl die Struktur als auch die Anschlußbelegung (vgl. Abschnitt 2.3. in Kapitel 2).

Hinweis:
Die Datenwegschaltkreise enthalten gleichartig aufgebaute RAMs als “Cache-Grundausstattung” (CY82C690: 8k · 64, CY82C692: 16k · 64)).

3.2.9. Cache-TAG-RAMs

TAG-RAMs sind spezielle SRAMs mit eingebautem Adreßvergleicher (Address Comparator). Daß es zweckmäßig ist, solche Schaltkreise anzubieten, ergibt sich aus folgenden Zusammenhängen:

- herkömmlicherweise (vgl. die Abbildungen 3.9 bis 3.15) sind die TAG-RAMs über ihre Datenanschlüsse mit dem Steuerschaltkreis verbunden. Dieser enthält den Adreßvergleicher. Das heißt, ein zeitkritischer Signalweg (Adressierung der TAG-RAM → Adreßvergleich → Entscheidung über Hit oder Miss) verläuft über Schaltkreisgrenzen hinweg. Die Folge: bei hohen Taktfrequenzen (50...66 MHz und mehr) gelingt es nicht mehr, die Hit/Miss-Entscheidung in jenem Taktzyklus zu treffen, zu dessen Beginn die Adresse übernommen wurde; daraus resultiert die Notwendigkeit, wenigstens einen Wartezustand einzufügen.
- die Auslegung auf Nutzung üblicher SRAMs (Kostenoptimierung) zwingt zu Kompromissen, z. B. zum Verzicht auf Kennzeichnungsbits,
- herkömmliche SRAMs als TAG-Speicher erfordern irgendeine Form der softwareseitigen Initialisierung nach dem Einschalten (Löschen von Kennzeichnungsbits bzw. Füllen mit gültigen Einträgen),
- mit üblichen SRAMs als TAG-Speicher kann man praktisch nur direktabbildende Caches kostengünstig verwirklichen (blockassoziative Organisationsformen würden einen beträchtlich höheren Aufwand erfordern - es sei denn, man baut den TAG-RAM in den Steuerschaltkreis ein (vgl. Abbildung 3.17)).
- solche Lösungen sind für eher einfache Konfigurationen (also: für PCs des Massen-Marktes) durchaus zweckmäßig, nicht aber für “richtige” Hochleistungssysteme (Server, Workstations usw.). Hier wird

vielmehr eine *leistungs*optimierte Struktur des TAG-RAM gefordert:

1. so breit wie notwendig: hohes Abbildungsvermögen bis hin zur "Cacheability" des gesamten linearen Adreßraumes (4 GBytes, bei Architekturen mit längeren Adressen - bis zu 64 Bits sind üblich - auch mehr).
2. soviele Kennzeichnungsbits wie notwendig: im besonderen *Multiprozessorsysteme* erfordern mehrere Kennzeichnungsbits. Will man z. B. das MESI-Protokoll implementieren, so müssen je Cache-Eintrag 4 Zustände gespeichert werden; in weiterentwickelten Protokollen (z. B. MOESI) sind noch mehr Zustände vorgesehen.
3. so schnell wie notwendig: bei Bus-Taktfrequenzen von über 66 MHz sollen keine zusätzlichen Wartezustände erforderlich sein.
4. bestmögliche Trefferraten: durch blockassoziative Cache-Organisation.

Im folgenden sollen Aufbau und Wirkungsweise anhand von 2 Beispielen kurz erläutert werden (Abbildungen 3.24 bis 3.30).

Abbildung 3.67 Der TAG-RAM IDT71B74 (IDT). Links: Blockschaltbild, rechts: Anschlußbelegung

Erklärung:
Wir zeigen zunächst einen älteren, vergleichsweise einfach aufgebauten Typ. Es handelt sich eigentlich um einen "gewöhnlichen" (asynchronen) 8k · 8-SRAM mit den üblichen Steuereingängen (/CS, /WE, /OE; vgl. Kapitel 1), der um einen Vergleichsschaltung (Comparator) erweitert ist und dessen Speicherzellen gemeinsam löschbar sind:

- Vergleichsfunktion: Ein Vergleichszugriff findet statt, wenn die Steuereingänge folgendermaßen belegt sind: /CS = Low, /WE = High, /OE = High. Die Datenausgänge sind dann hochohmig, und die Datenleitungen können mit den aktuellen (zu vergleichenden) Adreßbits belegt werden.
- Löschen (Rücksetzen): das Aktivieren der Leitung /RESET bewirkt ein Löschen aller Speicherzellen (die gesamte Speichermatrix hat danach den Inhalt Null; das erspart eine softwareseitige Initialisierung). Hierzu genügt ein /RESET-Impuls von ca. 50 ns Dauer.

Abbildung 3.68 Der TAG-RAM IDT71B74. Anwendungsbeispiel (IDT)

Erklärung:
Mit derartigen Schaltkreisen können verschiedenartige Cache-Anordnungen aufgebaut werden. Im Beispiel ist ein L2-Cache (Write Thru) für einen 486-Prozessor dargestellt. Zwei parallel betriebene TAG-RAM-Schaltkreise bilden eine TAG-Speicher mit 8k Einträgen zu 16 Bits. Die Vergleichssignale (MATCH) sind im Sinne des "Wired AND" zusammengeschaltet (es sind Open-Drain-Ausgänge). Eine Trefferanzeige (MATCH = High) ergibt sich somit nur dann, wenn in beiden RAMs die jeweilige Vergleichsbedingung erfüllt ist.

Bei "486-typischen" Cache-Einträgen von 16 Bytes reicht das Abbildungsvermögen für den vollen Adreßraum (4 GBytes) aus (in den TAG-Einträgen werden dafür sogar nur 15 Bits benötigt - vgl. die mit * gekennzeichnete Festbeschaltung). "Richtige" VALID-Bits gibt es nicht, der gesamte TAG-Speicher wird aber beim Rücksetzen auf Null gelöscht. Die mit der Eins (*) fest beschaltete Bitposition wirkt dann als eine Art Initialisierungs-Kennzeichen. Auch diese Bits sind anfänglich gelöscht. Bei den ersten Zugriffen wird nun der außen anliegende Festwert 1 mit der stets gespeicherten Null verglichen - infolge dessen ergibt sich stets ein Cache Miss. Mit dem Eintragen "gültiger"Adreßbits gelangt eine Eins auch in die Bitposition *, so daß künftige Vergleichszugriffe bei Gleichheit der Adreßbits Treffer signalisieren. (Die Behälter des Cache werden so gemäß den ausgeführten Speicherzugriffen nach und nach gültig - infolge der Festbeschaltung gibt es aber keine Möglichkeit, Einträge gezielt wieder ungültig zu machen. Der naheliegende Ausweg: Belegung der Bitposition * mit einem "echten" VALID-Bit, das von der

Cache-Steuerung eingetragen wird.)

Abbildung 3.69 Der TAG-RAM IDT71215 (IDT). Vereinfachtes Blockschaltbild

Erklärung:
Dies ist ein synchroner TAG-RAM mit 16k Einträgen, die aus 12 Adreß- (TAG-) und 3 Statusbits bestehen. Abbildung 3.27 zeigt weitere Einzelheiten (wobei es nicht erforderlich ist, alle Spitzfindigkeiten zu verstehen).

Abbildung 3.70 Der TAG-RAM IDT71215 (IDT). Ausführlicheres Blockschaltbild

Erklärung:

- alle Statusbits können über den /RESET-Eingang gleichzeitig auf Null gelöscht werden,
- es sind gesonderte Schreibzugriffe zu den TAG- und Statusbits möglich (Schreibsteuereingänge /WET, /WES),
- für die TAG-Bits sind bidirektionale Datenleitungen (TAG11...0) vorgesehen, für die Statusbits aber getrennte Ein- und Ausgänge (IN/OUT). Der Vorteil: (1) gespeicherte Statusbits können unmittelbar in der Cache-Steuerung wirksam werden, (2) die Cache-Steuerung kann neu gebildete Statusbelegungen sofort (im folgenden Taktzyklus) in den RAM eintragen.
- die Datenwege für TAG- und Stausbits werden über unabhängige Erlaubniseingänge gesteuert (OET, /OES),
- Schreibzugriffe werden voll synchron gesteuert (Flow-Thru-Organisation), Lese- und Vergleichszugriffe hingegen asynchron (Umschaltung über den Multiplexer (*) im Adressierungsweg). Der Vorteil asynchroner Zugriffe: geringste Reaktionszeiten auf Adreßänderungen.
- zur Nutzung der Statusbits: die Signalbezeichner legen eine bestimmte Nutzungsweise nahe (VLD = VALID, DTY = DIRTY, WT = WRITE THRU (um für ausgewählte Cache-Einträge selektiv das Write-Thru-Schreibverfahren erzwingen zu können). Grundsätzlich lassen sich die 3 Statusbits auf beliebige Weise belegen (beispielsweise um die 4 MESI-Zustände zu codieren).
- um unnötige Wartezustände zu vermeiden, muß die Cache-Steuerung zu Beginn eines jeden Zugriffs entscheiden, ob ein Treffer vorliegt oder nicht. Deshalb hat man vorgesehen, daß der TAG-RAM das entsprechende Signal (/BRDY bei den Intel-Prozessoren) aus der Vergleichsaussage (MATCH = Hit/Miss) heraus so zeitig wie möglich bilden kann. Die verschiedenen BRDY-Eingänge des Schaltkreises sind vorgesehen, damit die Systemsteuerung auf das BRDY-Signal einwirken kann (vgl. auch Abbildung 3.28).

Abbildung 3.71 Pentium-Prozessor mit Cache-Subsystem (IDT)

Erklärung:
Ein TAG-RAM IDT71215 bildet mit 2 synchronen Daten-RAMs den L2-Cache eines Pentium-Prozessors. Bei einer Cache-Größe von 256 kBytes ergibt sich bei 8k Einträgen und 12 Adreßbits Adreßbreite im TAG-RAM ein Abbildungsvermögen von 1 GByte.

Abbildung 3.72 Synchroner TAG-RAM in Pipelined-Burst-Organisation MCM69T618 (Motorola)

Erklärung:
Es handelt sich um einen vollsynchronen Schaltkreis (auch das Vergleichsergebnis wird synchron ausgewertet (siehe das Register vor dem MATCH-Ausgang). Der Speicher hat 64k Einträge zu 18 Bits. Es gibt keine Trennung zwischen TAG- und Statusbits. Die Nutzung der Bits ist Angelegenheit der Cache-Steuerung. Braucht man noch breitere Einträge, kann man mehrere Schaltkreise parallel betreiben. Die Pipelining-Organisation ermöglicht es, solche Speicher für Taktfrequenzen von 100 MHz (und mehr) zu bauen (bei der 100-MHz-Ausführung ist der

MATCH-Ausgang spätestens 5 ns nach der Low-High-Taktflanke gültig belegt).

Abbildung 3.73 Cache-Steuerschaltkreis mit eingebautem TAG-RAM IDT71V280 (IDT)

Erklärung:
Eine weitere Möglichkeit der Leistungssteigerung ist die Fortführung der Schaltungsintegration. Hier hat man einen TAG-RAM, der ähnlich organisiert ist wie der in den Abbildungen 3.26 und 3.27 gezeigte, mit einem Cache-Controller zusammengebaut. Der Schaltkreis ist für Pentium-Prozessoren optimiert. Als Datenspeicher können wahlweise asynchrone oder synchrone SRAMs eingesetzt werden (letztere wiederum in Flow-Thru- oder in pipelined-Organisation). Vorgesehene Cache-Größen: 256 oder 512 kBytes. 10 TAG-Bits ergeben bei 16k "pentium-typischen" Cache-Einträgen von 32 Bytes ein Abbildungsvermögen von maximal 2 GBytes, und 2 Statusbits genügen, um die 4 Zustände des MESI-Protokolls zu codieren.

3.3. Probleme der Cache-Erweiterung

3.3.1. Schaltungstechnik

Einfachste Speicheranordnungen bestehen aus einem einzigen Schaltkreis oder aus mehreren parallel angeordneten Schaltkreisen (einem Modul bzw. einer Bank). Reicht die so realisierbare Speicherkapazität nicht aus, so liegt es nahe, weitere Schaltkreise bzw. Speichermoduln (Banks) gleichsam hintereinanderzuschalten (Erweiterung "in der Tiefe"; Depth Expansion): der erste Schaltkreis bzw. die erste Speicherbank nimmt die ersten Datenworte (von Adresse 0 an) auf, der zweite Schaltkreis bzw. die zweite Speicherbank die nachfolgenden Datenworte usw. Die "hintereinandergeschalteten" Schaltkreise sind üblicherweise an einen gemeinsamen Datenbus angeschlossen. Moderne synchrone SRAMs haben mehrere Auswahleingänge (CE- bzw. CS-Anschlüsse), die es ermöglichen, Speichererweiterungen in üblichen Größenordnungen ohne jede zusätzliche Hardware vorzunehmen (Abbildung 3.31).

Abbildung 3.74 Speichererweiterung mit synchronen Burst-RAMs (BSRAMs)

Erklärung:

a) Speicheranordnung aus 2 Schaltkreisen bzw. Banks, die nacheinander adressiert werden. Zwei Schaltkreisauswahleingänge in konjunktiver Verknüpfung bilden praktisch in jedem Speicher einen eingebauten Adreßdecoder. Die Auswahladresse wird an den aktiv Low wirkenden Eingang /CE3 des ersten und an den aktiv High wirkenden Eingang CE2 des zweiten Schaltkreises angeschlossen. Die jeweils verbleibenden Eingänge (CE2, /CE3) werden so mit Festwerten beschaltet, daß die konjunktive Auswahlbedingung (CE2 = High & /CE3 = Low) erfüllt ist.

b) Speicheranordnung aus 4 Schaltkreisen bzw. Banks, die nacheinander adressiert werden. Hier besteht der eingebaute Adreßdecoder aus einer konjunktiven Verknüpfung von 4 Schaltkreisauswahleingängen (CS2.../CS5; vgl. auch Abbildung 3.23).

c) Struktur der Adresse. Die niedrigsten Adreßbits sind an die Adreßeingänge der Schaltkreise geführt. Bei einer Anordnung aus 2 Schaltkreisen bzw. Banks bildet das folgende Adreßbit die Erweiterungsadresse (Expansion Address EXAD), bei einer Anordnung aus 4 Schaltkreisen bzw. Banks sind es die beiden nachfolgenden Adreßbits (EXAD_H, EXAD_L).

3.3.2. Das Problem: Bus Contention

Der gemeinsame Datenbus ist üblicherweise ein Tri-State-Bus. An einem solchen Bus kann es Konflikte geben, wenn eine Einrichtung abschaltet (= ausgangsseitig hochohmig wird, also den Bus nicht mehr treibt) und eine andere Einrichtung aufschaltet (= aktiv wird und den Bus zu treiben beginnt). Bei Anordnungen gemäß Abbildung 3.31 ist sogar verstärkt damit zu rechnen, weil die Adressen direkt auf die Auswahleingänge wirken und es keine

Schaltmittel gibt, die ein gegenüber dem Abschalten verzögertes Aufschalten gewährleisten könnten. (Bussysteme, die Konflikte ohne weiteres aushalten - z. B. der Gunning-Bus -, sind beim aktuellen Stand der Technik nicht allgemein üblich.)

Maßgeblich für die Beurteilung möglicher Gefahren aus solchen Konfliktfällen (Bus Contention) sind folgende Datenblatt-Werte:

- die Abschaltzeit (Turn-off Time, "Output to High Z" t_{QHZ}),
- die Aufschaltzeit (Turn-on Time, "Output to Low Z" t_{QLZ}).

Der Konfliktfall ergibt sich, wenn der eine Schaltkreis noch aufgeschaltet hat, der andere Schaltkreis aber schon aufschaltet (Abschaltzeit > Aufschaltzeit; $t_{QHZ} > t_{QLZ}$). Die Dauer t_{CONT} des Konfliktfalls ergibt sich dann als Differenz:

$t_{CONT} = t_{QHZ} - t_{QLZ}$.

Offensichtlich gibt es keinen Konflikt, wenn die Schaltkreise schneller abschalten als aufschalten (Abschaltzeit < Aufschaltzeit: $t_{QHZ} < t_{QLZ}$ (Prinzip "Break before Make")). Die Durchsicht einschlägiger Datenblätter ergibt aber, daß diese Bedingung an sich nie erfüllt wird. Trotzdem gehen die Hersteller davon aus, daß man Schaltkreise in Konfigurationen ähnlich Abbildung 3.31 gefahrlos betreiben kann. Wir müssen uns hierzu das Datenblatt genauer ansehen:

- t_{QHZ} ist ein *Maximal*wert (der Schaltkreis braucht zum Abschalten schlimmstenfalls so lange, nämlich bei höchstzulässiger Betriebstemperatur und geringstzulässiger Betriebspannung, schaltet aber typischerweise schneller ab).
- t_{QLZ} ist ein *Minimal*wert (der Schaltkreis schaltet schlimmstenfalls so schnell auf, nämlich bei geringstzulässiger Betriebstemperatur und höchstzulässiger Betriebsspannung, braucht aber typischerweise mehr Zeit (die Begrenzung "nach oben" ergibt sich aus der jeweiligen Zugriffszeitspezifikation)).

Nun werden die gegeneinander kämpfenden Schaltkreise in der Praxis typischerweise unter gleichen Bedingungen betrieben (gleiche Betriebstemperatur, gleiche Versorgungsspannung). Eventuelle Konflikte sind deshalb so kurz (1 ns oder weniger), daß sie nicht schaden.

Das gilt allerdings nur, wenn es sich um Schaltkreise gleichen Typs handelt.

Vorsicht ist aber geboten, wenn beispielsweise ein Motherboard, das mit Schaltkreise des Typs X bestückt ist, z. B. mit einem Speichermodul erweitert werden soll (vgl. Abbildung 3.3a), das Schaltkreise des Typs Y (womöglich eines anderen Anbieters) enthält. Diese Gefahr war Anlaß, spezielle Varianten der Pipelined-Burst-RAMs (PBSRAMs) einzuführen. Die Unterschiede werden durch die Begriffe "Double Cycle Deselect" (DCD) und "Single Cycle Deselect (SCD) bezeichnet.

3.3.3. Double Cycle Deselect (DCD) und Single Cycle Deselect (SCD)

Der "herkömmliche" Pipelined-Burst-RAM (PBSRAM) ist ein DCD-RAM. Abbildung 3.32 zeigt das grundsätzliche Verhalten beider Auslegungen in der Gegenüberstellung, und zwar anhand eines sozusagen "bilderbuchmäßigen" Ablaufs (vgl. Kapitel 2, Abschnitt 2.2.3.8.) ohne Konfliktfälle.

Abbildung 3.75 PBSRAMs im Vergleich: DCD und SCD in einem Burst-Lesezyklus

Erklärung:

Die Abbildung zeigt einen einzelnen Burst-Leszyklus, der mit /ADSP = Low und /CE1 = Low gestartet wird. Nach den 4 Lesezugriffen soll der Speicher wieder deselektiert werden. Hierzu wird die Signalkombination /ADSC = Low und /CE1 = High verwendet (vgl. Tabelle 2.12 in Kapitel 2, Abschnitt 2.2.3.8.).

a) DCD-Organisation. Infolge der Pipelining-Organisation muß dieser "Befehl" (Deselektieren) mit einem Taktzyklus Vorlauf gegeben werden, also in dem Taktzyklus an den Schaltkreiseingängen anliegen, in dem das letzte Datenwort (4.) ausgegeben wird (*). Im wiederum folgenden Taktzyklus wird dann der Speicher deselektiert. (Mit anderen Worten: das DCD-Verhalten ist sozusagen der "Nebeneffekt" einer strikten Pipelining-Organisation - alle Steuerwirkungen an den Eingängen machen sich mit einem Takt Verzögerung an den Ausgängen bemerkbar.)

b) bei der SCD-Organisation hat man nun für den Deselektionsablauf das Pipelining aufgehoben: die Deselect-Funktion wirkt hier bereits im aktuellen Zyklus - wie bei einem Flow-Thru-Speicher. (Liegt vor der Low-High-Flanke des Taktes die entsprechende Signalkombination an den Eingängen, so wird sofort nach dieser Taktflanke deselektiert.) Steuert man einen SCD-PBSRAM gemäß Abbildung an, so könnte man nur 3 Worte lesen.

Hinweis:
Ein Deselektieren kann man in PBSRAMs auf zweierlei Weise auslösen (vgl. auch Tabelle 2.12):

1. mit /CE1 = High und /ADSC = Low (wie in Abbildung 3.32 gezeigt),
2. mit /ADSP = Low und Nicht-Auswahl über CE2, /CE3 usw. Der Schaltkreis geht in den Deselect-Zustand über, wenn er nicht ausgewählt ist, aber /ADSP aktiv wird. Auch dieses Deselektieren wird bei DCD einen Takt später und bei SCD im selben Takt wirksam (wichtig für das Verständnis der Abbildungen 3.33 und 3.34).

3.3.4. Speichererweiterung mit DCD-RAMs

Abbildung 3.33 zeigt, daß DCD-RAMs das lückenlose Aneinanderreihen von Lesezugriffen gestatten (vgl. auch Abbildung 2.24 in Kapitel 2, Abschnitt 2.2.3.5.).

Abbildung 3.76 Aufeinanderfolgende Lesezugriffe mit Bank-Übergang (DCD)

Erklärung:
Der Ablauf betrifft eine Konfiguration aus 2 Banks mit je 8k Cache-Einträgen zu 256 Bits = 32 Bytes (das ist eine für Pentium-Systeme typische Konfiguration eines 512 kBytes großen L2-Caches). Die Adreßbits werden folgendermaßen genutzt: 4...0: Byte im Eintrag, 17...5: Eintrag in Schaltkreis, 18: Schaltkreisauswahl (Adreßbit 18 entspricht der Adreßleitung EXAD in Abbildung 3.31). Wir zeigen hier 2 aufeinanderfolgende Burst-Lesezyklen, wobei der erste Zyklus auf die erste und der nachfolgende Zyklus auf die zweite Speicherbank zugreift.

a) der erste Burst-Lesezyklus wird gestartet (Anfangsadresse A). Es handelt sich um den an sich bekannten Ablauf (vgl. Abbildung 2.27 in Kapitel 2, Abschnitt 2.2.3.8.).

b) hier wird der zweite Burst-Lesezyklus gestartet (Anfangsadresse B), und zwar mit einem Takt Vorlauf, so daß die gelesenen Daten lückenlos aufeinanderfolgen,

c) die Anfangsadresse B hat aber gegenüber der Adresse A eine andere Belegung des Adreßbits A18. Damit wird (1) die Speicherbank X abgeschaltet (d. h. mit /ADSP = Low und Nicht-Auswahl infolge A18 = High zum Zeitpunkt b) deselektiert) - und (2) die Speicherbank Y angeschaltet (d. h. mit /ADSP = Low und Auswahl infolge A18 = High zum Zeitpunkt b) selektiert). Deselektion von Bank X und Selektion von Bank Y werden einen Taktzyklus nach b) wirksam. Dies geschieht taktsynchron und lückenlos, so daß die Gefahr von Bus Contention gegeben ist (!).

d) hier ist nochmals der alternative Deselektionsablauf (/ADSC = Low, /CE1 = High) dargestellt (vgl. Abbildung 3.32).

3.3.5. Speichererweiterung mit SCD-RAMs

Der Zweck der SCD-Organisation besteht darin, im Fall des Falles (Übergang von einer Speicherbank zur anderen) einen Taktzyklus freizulassen, um Buskonflikte mit Sicherheit auszuschließen (Abbildung 3.34).

Abbildung 3.77 Aufeinanderfolgende Lesezugriffe mit Bank-Übergang (SCD)

Erklärung:
Das Szenarium entspricht jenem von Abbildung 3.33.

a) der erste Burst-Lesezyklus wird gestartet (Anfangsadresse A). Es handelt sich um den an sich bekannten Ablauf (vgl. Abbildung 2.27 in Kapitel 2, Abschnitt 2.2.3.8.).

b) hier wird der zweite Burst-Lesezyklus gestartet (Anfangsadresse B), im Gegensatz zum DCD-RAM aber nicht mit einem Takt Vorlauf. Wir müssen 4 Worte lesen (vollständiger Burst-Zyklus). Da ein SCD-Speicher mit /ADSP = Low und Nicht-Auswahl (wegen A18 = High) sofort deselektiert wird, können wir nicht schon dann deselektieren, wenn das 3. Wort auf dem Datenbus liegt (vgl. die Abbildungen 3.32, 3.33), sondern wir müssen das Deselektieren auf den folgenden Taktzyklus verschieben.

c) infolge der SCD-Organisation wird die Speicherbank X nach der Low-High-Taktflanke b) sofort deselektiert. Gleichzeitig wird (mit /ADSP = Low und Auswahl mit A18 = High) in Speicherbank Y der folgende Burst-Zyklus gestartet. Infolge der Pipelining-Organisation erscheinen aber die gelesenen Daten erst einen Taktzyklus später an den Ausgängen, so daß der Datenbus für nahezu eine Taktperiode unbelegt bleibt. Dies genügt, um Buskonflikte sicher zu vermeiden.

d) hier ist nochmals der bekannte Deselektionsablauf (/ADSC = Low, /CE1 = High) dargestellt (vgl. Abbildung 3.32).

Hinweise:

1. Die Betriebsweise (DCD oder SCD) ist eine Eigenschaft des Schaltkreises. Die Hersteller bieten üblicherweise Grundtypen (z. B. 32k · 32 für 66 MHz) in beiden Ausführungen an. Beim Bestellen achtgeben!
2. SCD ist Bestandteil der Intel-BSRAM-Spezifikation (das ist eine Art Lastenheft der Fa. Intel, das besagt, wie Burst-RAMs auszulegen sind, damit sie zu den Intel-Schaltkreissätzen passen).
3. DCD gewährleistet höchstes Leistungsvermögen. Zwei aufeinanderfolgende Burstzyklen können auch beim Übergang von einer Bank auf die andere nach dem Taktschema 3-1-1-1-1-1-1-1 ausgeführt werden (8 Worte werden in 10 Takten gelesen).
4. SCD führt demgegenüber beim Übergang von einer Bank auf die andere zu einem Taktschema 3-1-1-1-2-1-1-1 (8 Worte in 11 Takten).
5. Bei aufeinanderfolgenden Burstzyklen innerhalb derselben Bank ermöglicht auch SCD das Zugriffe im Taktschema 3-1-1-1-1-1-1-1. Da der Speicher nicht deselektiert wird (bei /ADSP = Low bleibt er ausgewählt), kann man /ADSP genauso aktivieren wie beim DCD-RAM (vgl. b) in Abbildung 3.32) - ohne Deselektieren verhält sich die Pipeline beider Speichertypen gleichartig.
6. Weshalb nimmt man nicht nur DCD-Typen und schiebt bei Bank-Wechsel einfach einen Deselect-Zyklus ein? - Es würde funktionieren, nur hätte dies an anderen Stellen Schwierigkeiten oder Leistungseinbußen zur Folge oder es würde Änderungen in der RAM-Ansteuerung erfordern (neue Steuersignale usw.) Entscheidend ist vielmehr die Entwicklungsgeschichte: das Ansteuerschema über /ADSP und /ADSC war bereits zum Industriestandard geworden. Nun wollte man die L2-Caches durch zusätzliche Speichermoduln erweiterbar gestalten. Also mußte eine Lösung gefunden werden, Buskonflikte (infolge der Bestückung mit den “unmöglichsten” Schaltkreiskombinationen) zu vermeiden. Eine brauchbare Lösung muß sich aber in das Bestehende einfügen - und SCD ist eine solche Möglichkeit.

7. *DCD- und SCD-Typen durch Testen erkennen.* Hierzu kann man von Abbildung 3.32 ausgehen: (1) in den Speicher einen vollständigen Eintrag (z. B. 4 Worte) schreiben, wobei jedes Wort einem anderen Bitmuster entspricht (z. B. 11...1H, 22...2H, 55...5H, AA...AH). (2) einen Lese-Burstzugriff mit anschließendem Deselektieren so ausführen, wie dies in Abbildung 3.32 für den DCD-Typ dargestellt ist. Handelt es sich tatsächlich um einen DCD-Typ, so werden alle 4 Einträge korrekt zurückgelesen. Ein SCD-Typ liefert hingegen nur die ersten 3 Worte zurück (das 4. entspricht dann typischerweise dem 3. - da der hochohmige Bus die letzte Belegung beibehält). (Manche BIOS-Schaltkreissatz-Kombinationen prüfen so; es ist aber auch damit zu rechnen, daß entsprechende Jumper oder Wahlmöglichkeiten im BIOS-Setup vorgesehen sind.)
8. Zu den Steuerschaltkreisen. Es ist mit verschiedenen Auslegungen zu rechnen:

   - der Schaltkreissatz ist auf den BSRAM-Standard von Intel festgelegt. Hier sind nur SCD-Typen einsetzbar.
   - der Schaltkreissatz kann sowohl DCD- aus auch SCD-Typen steuern, sieht aber beim Wechseln zwischen 2 Banks immer einen “Leerzyklus” vor.
   - der Schaltkreissatz kann sowohl DCD- aus auch SCD-Typen steuern, bietet aber die Möglichkeit, DCD-Typen im schnellstmöglichen Taktschema (3-1-1-1-1-1-1) zu betreiben.

3.4. Cache-Moduln

3.4.1. Konstruktive Ausführung

Cache-Moduln für Personalcomputer sind typischerweise als DIMM (Dual in Line Modules) ausgeführt, das heißt, die mechanische Grundlage bildet ein Streifen aus Glasfaser-Epoxyd-Leiterplattenmaterial mit einem 2-reihigen direkten Steckverbinder. Zwei Arten von Steckverbindern gelten praktisch als Industriestandard (Tabelle 3.19).

Ausführung und Anschlußzahl	Leiterplatten-Abmessungen (in mm, gerundet)	Anwendung	Steckverbindertypen (Beispiele)
SODIMM (Small Outline DIMM); 0,8 mm Anschluß-abstand (Pitch), 144 Anschlüsse	68 · 25	Cache-Moduln für portable PCs	AMP C-316310-2
DIMM; 1,27 mm (= 50 mil) Anschlußabstand (Pitch), 160 Anschlüsse	■ 110 · 29, ■ 110 · 33	Cache-Moduln für ortsfeste PCs	BURNDY CELP2X80SC3Z48

Tabelle 3.19 Cache-Moduln (Übersicht)

3.4.1.1. Bauformen

Es gibt eine beachtliche Typenvielfalt. Solche Moduln sehen sich auf den ersten Blick oft zum Verwechseln ähnlich, sind aber keineswegs immer gegeneinander austauschbar. In der Servicepraxis kann es gelegentlich notwendig sein, bestimmte Ausführungen sicher zu erkennen:

1. ein gegebenes Motherboard ist zu erweitern. Welche Modul-Typen sind hierfür geeignet?
2. es liegen Moduln auf Lager - natürlich nicht so gekennzeichnet, daß man gleich sieht, worum es sich handelt.

Wir geben zunächst anhand der Abbildungen 3.35 bis 3.38 einen Überblick über verbreitete Bauformen. Nähere

Einzelheiten erklären wir weiter unten anhand von Beispielen.

Abbildung 3.78 Die Abmessungen eines SODIMM-Moduls mit 144 Anschlüssen (IDT). Alle Maßangaben in mm. Zur Anschlußbelegung siehe weiter unten Abschnitt 3.4.2.1.

Abbildung 3.79 Die Abmessungen eines DIMM-Moduls mit 160 Anschlüssen (Cypress). Maßangaben in Zoll und mm. a) Vorderansicht, b) Seitenansicht bei einseitiger Bestückung, c) Seitenansicht bei doppelseitiger Bestückung

Erklärung:

1) Datenspeicher (synchrone Burst-RAMs),
2) TAG-Speicher (asynchroner SRAM).

Moduln mit 256 kBytes sind typischerweise einseitig, Moduln mit 512 kBytes oft doppelseitig bestückt.

Zur Bauhöhe: es sind zwei Ausführungen üblich: (1) ca. 29 mm (1,13...1,14"), (2) ca.33 mm (1,3 “). Nachsehen, welche Einbauhöhe im PC noch annehmbar ist.

Abbildung 3.80 DIMM-Modul mit asynchronen Daten-RAMs und Pegelwandlung auf 3,3 V (Cypress). a) Vorderansicht, b) Seitenansicht, c) Rückansicht. Siehe weiterhin Abschnitt 3.4.2.2.

Erklärung:

1) TAG-RAM für DIRTY-Bit,
2) Adreßregister (Latch),
3) Daten-RAMs,
4) Pegelwandler 5 V → 3,3 V,
5) TAG-RAM für Adreßbits.

Abbildung 3.81 DIMM-Moduln gemäß COASt-Standard (Cypress). a) 256 kBytes, 11 TAG-Bits, b) 512 kBytes, 8 TAG-Bits. Es ist jeweils die Vorder- und die Rückansicht dargestellt. Siehe weiterhin Abschnitt 3.4.2.5.

Erklärung:

1) Datenspeicher (synchrone Burst-RAMs),
2) TAG-RAM für Adreßerweiterung (3 zusätzliche Adreßbits),
3) TAG-RAM Grundausstattung (8 Adreßbits),
4) Serienwiderstände in den Datenleitungen (Dünnfilm-Moduln mit je 8 Widerständen; Richtwerte: 10...22 Ω),
5) Freifläche (unbestückt) für Position 2 (TAG-Adreßerweiterung).

3.4.1.2. Anschlußbelegungen 160-poliger DIMMs

In Abbildung 3.39 haben wir die Anschlußbelegungen verbreiteter Cache-Moduln zusammengestellt. Es handelt sich hier ausnahmslos um Moduln mit 64 Bits Datenwegbreite, wie sie für PCs mit Pentium-Prozessoren benötigt werden.

Abbildung 3.82 Anschlußbelegungen 160-poliger DIMMs im Vergleich (Ansicht von oben)

Erklärung:
Die Cache-Moduln sind typischerweise für bestimmte Schaltkreissätze vorgesehen:

a) Cache-Moduln für den OPTi-Viper-Schaltkreissatz (siehe weiterhin Abschnitt 3.4.2.2.),
b) Cache-Moduln für den Intel-"Neptune"-Schaltkreissatz (82430NX; siehe weiterhin Abschnitt 3.4.2.3.),
c) Cache-Moduln mit eingebautem Cache Controller (siehe weiterhin Abschnitt 3.4.2.4.),
d) Cache-Moduln gemäß COASt-Standard (siehe weiterhin Abschnitt 3.4.2.5.),
e) Cache-Moduln gemäß COASt-Standard mit DRAM-Caches (Fusion Memory bzw. MCache). Bis auf die speziellen Anschlüsse zum Betrieb der DRAM-Anordnung (vgl. Abbildung 2.34 und Tabelle 2.23 in Kapitel 2, Abschnitt 2.4.2.) unterscheiden sie sich praktisch nicht von den "gewöhnlichen" COASt-kompatiblen Moduln).

3.4.1.3. Cache-Moduln voneinander unterscheiden

Vielfach genügt es, sich charakteristische Masse- und Speisespannungsanschlüsse anzusehen, um zu erkennen, um welche Art von Modul es sich überhaupt handelt (Tabelle 3.20). Ist dies erst einmal bekannt, könnte man sich die Belegung der Erkennungsanschlüsse (PD = Presence Detect) ansehen (vgl. dazu die Tabellen 3.22 bis 3.27). Ist der Hersteller bekannt, könnte man im Datenmaterial nachsehen (Internet) und erforderlichenfalls weitermessen. So ist die installierte Speicherkapazität durch Verfolgen der höherwertigen Adreßleitungen erkennbar (Beispiel: wird Adreßleitung A18 an Schaltkreiseingänge geführt, so handelt es sich um 512 kBytes).

Praxistips:

1. Durchgangsprüfung: grundsätzlich in stromlosen Zustand. Prüfspannung < 0,5 V. ESD-Vorkehrungen beachten! (Vgl. auch die Ausrüstungs-Übersicht, Abschnitt 2.1.9.)
2. Messen auf dem Motherboard: (1) Masseverbindungen, Adressen usw. mittels Durchgangsprüfung in stromlosem, Speisespannungen in eingeschaltetem Zustand prüfen.
3. Speichermoduln werden fast durchweg mit Schaltkreisen bestückt, die Industriestandards sind (z. B. mit PBSRAMs 32k · 32). Die Anschlußbelegungen sind aus dem einschlägigen Datenmaterial ersichtlich, wobei es auf den Hersteller im einzelnen nicht ankommt (die Suche nach Datenmaterial kann abgebrochen werden, wenn man das erste passende Datenblatt gefunden hat - machmal hilft auch der Standard JESD 21-C). Achtung: Die Rückseiten der Moduln sind gelegentlich (aber nicht immer) mit Schaltkreisen bestückt, die ein spiegelverkehrtes Anschlußbild haben.

Modul-Typen	Unterscheidungsmerkmale (Auswahl)
Cache-Moduln für den OPTi-Viper-Schaltkreissatz (Abbildung 3.39a)	■ Pin 160 an + 5 V, Pin 30 an + 3,3 V (die anderen Typen: Masse), ■ Pins 150 und 70 an Masse, ■ Pin 92 an + 5 V, Pin 12 an + 3,3 V
Cache-Moduln für den Intel-"Neptune"-Schaltkreissatz (Abbildung 3.39b)	■ Pins 143 und 63 an Masse, ■ Pin 158 an + 5 V, Pin 78 an + 3,3 V, ■ Pins 93 und 13 an Masse Siehe auch die Hinweise zu Abbildung 3.47 (Erkennung, ob das Modul einen Adreß-Latch enthält oder nicht).

Cache-Moduln mit eingebautem Cache Controller (Abbildung 3.39c)	■ Pins 23, 87, 117 und 155 an Speisespannung, ■ Pins 90 und 10 an Masse, ■ Pins 152 und 72 an Masse
Cache-Moduln gemäß COASt-Standard (Abbildung 3.39d)	■ Pin 156 an + 5 V, Pin 76 an + 3,3 V, ■ Pins 144 und 64 an Masse, ■ Pins 117 und 37 an Masse, ■ Pins 132 an + 5 V, Pin 52 an + 3,3 V Siehe auch die Hinweise zu Abbildung 3.50 (Erkennung von SRAM-Moduln mit COASt-Pinout).
Cache-Moduln gemäß COASt-Standard mit DRAM-Caches (Abbildung 3.39e)	gleiche Anschlußbelegung wie die "statischen" COASt-Moduln. Bei letzteren unbeschaltete (NC) Anschlüsse sind hier aber folgendermaßen belegt: ■ Pin 97: F0, ■ Pin 100: RESET#, ■ Pin 111: H/WR#.

Tabelle 3.20 Meßtechnische Anhaltspunkte zum Erkennen von Modul-Typen

3.4.1.4. Qualitätsmerkmale

Cache-Moduln unterscheiden sich im Preis, aber auch in der Qualität (Abbildung 3.40, Tabelle 3.21).

Abbildung 3.83 Qualitätsmerkmale von Cache-Moduln (Erklärung in Tabelle 3.21)

Merkmal (vgl. Abbildung 3.40)	gut	schlecht
1) Leiterplatte	Mehrlagenplatine (6 Ebenen sind typisch) mit gesonderten Ebenen für Masse und Speisespannung	keine gesonderten Ebenen für Masse und Speisespannung
2) Schaltkreise	erfüllen die Zugriffszeit-Spezifikationen mit genügend Sicherheitszuschlag, Hersteller und Typ deutlich erkennbar	Zugriffszeit-Spezifikationen werden nur knapp oder gar nicht erfüllt, Hersteller- und Typangaben nicht erkennbar
3) Leiterplatten-gestaltung, Stütz-kondensatoren	"HF-gerechte" Auslegung (kurze Leiterzüge)[1)], genügend Stütz-kondensatoren (z. B. einer je V_{CC}-Schaltkreisanschluß), Serienwiderstände in den Datenleitungen[2)]	"gleichstrommäßige" Auslegung (kreuz und quer, verschnörkelt usw.), wenige Stützkondensatoren
4) Steckkontakte	Goldauflage wenigstens 0,03 mil (0,7 Tausendstel mm)[3)]; typischerweise über 0,15 mil (ca. $^4/_{1000}$ mm) Nickel	Goldauflage gerade mal 0,01 mil ("Gold Flash", d. h. wirklich nur ein Hauch von 0,25 Tausendstel mm)

5) Unterkante der Kontaktreihe	entgratet (Tapered Edge = mit einer gewissen Fase; läßt sich leicht stecken)	mit Grat (läßt sich nur schwer stecken)[4)]

1): die COASt-Spezifikation schreibt für die Leiterzüge einen definierten Wellenwiderstand von 70 Ω vor; 2): siehe folgenden Abschnitt; 3): in COASt-Standard gefordert; 4): siehe folgenden Praxistip

Tabelle 3.21 Qualitätsmerkmale von Cache-Moduln

3.4.1.5. Serienwiderstände in den Datenleitungen

Diese Vorkehrung dient dazu, Reflexionserscheinungen (Undershoot, Ringing) auf den Datenleitungen zu unterdrücken. Kritisch sind vor allem Über- und Unterschwinger im Low-Pegel (positive Spitzen können die TTL-Schaltschwelle überschreiten, negative Spitzen eine unzulässig große Amplitude erreichen; Abbildung 3.41).

Abbildung 3.84 Signale auf Datenleitungen (nach: Corsair Microsystems). a) Cache-Modul ohne, b) mit Serienwiderständen

Erklärung:
Solche Effekte treten vor allem dann auf, wenn besonders schnelle Ausgangsstufen (z. B. die von PBSRAMs) lange Leitungen treiben. Ein Ausweg: näherungsweise Anpassung an den Wellenwiderstand der Leitungen durch Einfügen von Serienwiderständen. Typische Widerstandswerte liegen zwischen 10 und 22 Ohm, wobei meist je 8 Widerstände in einem Dünnfilm-Netzwerk zusammengefaßt sind (vgl. auch Position 4 in Abbildung 3.38). Es gibt (ansonsten gleichartige) Moduln mit und ohne Serienwiderstände (wobei letztere merklich teurer sind). Sind die Datenleitungen hinreichend kurz, arbeiten auch Moduln ohne Serienwiderstände befriedigend.

Praxistips:

1. Ein Modul mit Serienwiderständen als Prüfhilfe bereithalten (zum Nachweisen, ob an zeitweiligen Fehlfunktionen das Cache-Modul schuld ist).
2. Serienwiderstände - vor allem auch die Lötverbindungen - sollten im Problemfall (Aussetzfehler, Fehler in einzelnen Bits usw.) gebührend verdächtigt werden (Durchgangsprüfung von den Schaltkreis- zu den Modulanschlüssen). Womöglich läßt sich ein - doch nicht ganz billiges - Modul durch eine vergleichsweise unproblematische Reparatur retten (Nachlöten oder Widerstandsnetzwerk tauschen).

3.4.2. Ausführungsbeispiele

3.4.2.1. Beispiel 1: SODIMM-Modul für portable PCs mit Pentium-Prozessor

Die Cache-Moduln IDT7MPV6271 enthalten Pipelined-Burst-SRAMs als Daten- und einen asynchronen SRAM als TAG-Speicher (Abbildung 3.42; zur Bauform siehe Abbildung 3.35).

Abbildung 3.85 Cache-Moduln IDT7MPV6271 (IDT). a) Blockschaltbild, b) Anschlußbelegung (Ansicht von oben), c) Signal-Übersicht

Erklärung:
Das dargestellte Modul bildet einen Cache von 256 kBytes. Es enthält nur die Speicherschaltkreise. Der TAG-RAM kann wahlweise mit 8 Adreßbits oder mit 7 Adreßbits und einem DIRTY-Bit belegt werden (deshalb die Anschlußbezeichnung TAG_7/DIRTY). Die PBSRAMs werden in Byte-Write-Organisation betrieben (es sind lediglich die byteweisen Schreiberlaubnissignale über die Anschlüsse geführt).

Derartige Moduln sind zum Einsatz in reinen 3,3V-Umgebungen bestimmt und haben deshalb keine Anschlüsse für 5 V Speisespannung. Es sind 2 Erkennungssignale (Presence Detect) vorgesehen (Tabelle 3.22). Zur Auswertung solcher fest belegten Signale vgl. Abbildung 1.28 in Kapitel 1, Abschnitt 1.5..

PD1 (Anschluß 142)	PD0 (Anschluß 141)	Bedeutung
NC	NC	kein Modul installiert
NC	GND	256 kBytes Pipelined Burst (im Beispiel = IDT7MPV6271)
GND	NC	reserviert für weitere Ausführungen
GND	GND	

Tabelle 3.22 SODIMM-Cache-Moduln: Erkennungssignale (Presence Detect)

Hinweis:
Von manchen Moduln gibt es verschiedene Ausführungen, die sich in der Geschwindigkeit der TAG- und der Daten-RAMs unterscheiden (es gibt auch Bauformen, die bei Bestückung mit gleich schnellen Daten-RAMs verschieden schnelle TAG-RAMs enthalten). Geschwindigkeits-Beispiele (nach IDT): Zugriffszeit der Daten-RAMs (Taktflanke zu Datenausgang): 7 ns; TAG-RAM-Zugriffszeiten: 12 oder 15 ns. Bestellbezeichnungen genau ansehen und mit den Typenlisten/Datenblättern vergleichen (Internet).

3.4.2.2. Beispiel 2: DIMM-Moduln für den OPTi-Viper-Schaltkreissatz

Solche Moduln gibt es in 3 Ausführungen: (1) mit asynchronen SRAMs, (2) mit Flow-Thru-Burst-RAMs, (3) mit Pipelined-Burst-RAMs (Abbildungen 3.43, 3.44). Der TAG-Speicher ist mit asynchronen SRAMs aufgebaut; er besteht aus einem Schaltkreis in · 8-Organisation für die TAG-Adresse und einem in · 1-Organisation für das DIRTY-Bit. Zur Anschlußbelegung siehe Abbildung 3.39a.

Abbildung 3.86 Cache-Modul mit asynchronen SRAMs und Pegelwandlung 5 V → 3,3 V (Cypress)

Erklärung:
Die Abbildung zeigt eine spezifisch kostenoptimierte Auslegung: es werden preisgünstige 5-V-SRAMs eingesetzt, und die Ausgangspegel werden in 3.3-V-Signale gewandelt. Hierfür dienen CMOS-Schalterbauelemente (vgl. auch Position 4 in Abbildung 3.37). Der CBUS3384 ist ein Bus-Schalter für 10 Bitpositionen. Er wird hier fest als "Durchreiche" betrieben. Der Effekt: beim Durchgang erfahren Signale, deren Pegel nahe an der Speisespannung liegt, einen Spannungsabfall von etwa 1 V, bezogen auf die Speisespannung des Schaltkreises. Diese wird hier über eine Zenerdiode bereitgestellt und beträgt 4,3 V - so daß sich ausgangsseitig die gewünschten 3,3 V ergeben. (Eingangsseitige Pegel bis zu ca. 3,5 V werden unverändert durchgereicht, so daß 3,3-V-Signale vom Datenbus direkt an den (TTL-kompatiblen) RAM-Anschlüssen erscheinen.) Es gibt auch Moduln, die mit 3,3-V-SRAMs bestückt sind und deshalb keine Pegelwandlung brauchen.

Abbildung 3.87 Cache-Modul mit synchronen Burst-SRAMs (Cypress)

Hinweise:

1. Den asynchronen Daten-RAMs ist ein Adreß-Halteregister vorgeschaltet (Address Latch; vgl. Position 2 in Abbildung 3.37). Es ersetzt praktisch das eingebaute Adreßregister der synchronen RAMs.
2. Die synchronen RAMs werden in Byte-Write-Organisation betrieben.
3. Steuersignalanschlüsse werden je nach RAM-Bestückung (asynchron oder synchron) unterschiedlich belegt (vgl. Abbildung 3.39a).

4. Zur TAG-Größe: bei 256 kBytes 8k · 8 + 8k · 1 (Bestückung meist 16k · 1), bei 512 kBytes 16k · 8 (Bestückung auch 2 · 8k · 8 oder 1 · 32k · 8) + 16k · 1. Manchmal findet man auch ausschließlich 32k · 8-Typen (die infolge der Massenfertigung gelegentlich billiger sind als SRAMs mit geringerer Kapazität).
5. Zu den Erkennungssignalen siehe Tabelle 3.23.

Presence-Detect-Signale				Bedeutung
PD3[1)]	PD2[1)]	PD1[2)]	PD0[2)]	
NC	NC	NC	NC	kein Modul installiert
NC	NC	GND	GND	asynchron, 256 kBytes
NC	GND	GND	GND	asynchron, 512 kBytes
NC	NC	NC	GND	Flow Thru Burst, 256 kBytes
NC	GND	NC	GND	Flow Thru Burst, 512 kBytes
NC	NC	GND	NC	Pipelined Burst, 256 kBytes
NC	GND	GND	NC	Pipelined Burst, 512 kBytes

1), 2): siehe Erklärung im Text

Tabelle 3.23 Erkennungssignale (Presence Detect)

Erklärung:

1) PD3, PD2 codieren die Speicherkapazität: NC, NC = 256 kBytes; NC, GND = 512 kBytes,
2) PD1, PD0 codieren die Speicherbestückung: GND, GND = asynchron; NC, GND = Flow Thru Burst; GND, NC = Pipelined Burst

3.4.2.3. Beispiel 3: Cache-Moduln für den Intel-"Neptune"-Schaltkreissatz

Die Steuerschaltkreise 82434LX/NX haben einen eingebauten TAG-RAM. Deshalb enthalten einschlägige Cache-Moduln nur den Datenspeicher. Dieser kann mit asynchronen oder mit Flow-Thru-Burst-RAMs aufgebaut werden (Abbildungen 3.45, 3.46).

Abbildung 3.88 L2-Cache (256 kBytes) mit asynchronen SRAMs und Steuerschaltkreis (PCMC) 82434LX/NX (Intel)

Erklärung:

1) die höherwertigen Bits der Datenadresse werden in einem externen Adreßregister (Address Latch) gehalten (HA = Adresse vom Prozessorbus (Host Address)),
2) der Steuerschaltkreis liefert die 4 niedrigstwertigen Adreßbits. Die 2 niedrigstwertigen Bits dienen zur Auswahl des 64-Bit-Wortes aus dem Cache-Eintrag von 4 Worten (bei asynchronen RAMs muß der Steuerschaltkreis die Adresse gemäß Burst-Zählweise liefern). Das 3. Bit kann verwendet werden, um einen Interleaving-Betrieb mit 2 Speicherbanks zu implementieren. (Ansonsten hat die Aufteilung der Adresse den Vorteil, daß das externe Adreßregister nur 16 Bits breit sein muß - man kommt also mit 2 8-Bit-Schaltkreisen (oder einem 16-Bit-Typ aus.)
3) Verbindung fehlt beim 82343LX. Der 82343NX hat zwei weitere Ausgänge CCS1, 0 (jeder betrifft ein 32-Bit-Wort), die mit den CS-Eingängen der Speicherschaltkreise verbunden sind.

Abbildung 3.89 L2-Cache (512 kBytes) mit synchronen Burst-SRAMs (Flow-Thru-Organisation) und Steuerschaltkreis (PCMC) 82434LX/NX (Intel)

Erklärung:

1) der 82343LX erfordert stets ein externes Adreßregister. Der 82343NX kann wahlweise (durch Laden des Cache-Steuerregisters) entweder auf LX-Kompatibilität oder auf eine alternative Betriebsart (NX SRAM Connectivity) geschaltet werden. In dieser Betriebsart entfällt das externe Adreßregister, und die Adreßeingänge der SRAMs werden direkt an die Adreßleitungen des Prozessorbus angeschlossen.
2) die Verbindung ist nur beim LX (bzw. bei LX-Kompatibilität) vorgesehen. Bei aktivierter NX SRAM Connectivity sind auch diese 4 Adreßeingänge der RAMs direkt an die Adreßleitungen des Prozessorbus angeschlossen.
3) ADSP wird beim LX (bzw. bei LX-Kompatibilität) nicht verwendet (die RAMs werden über das Adreßregister adressiert, also nicht direkt vom Prozessor, und die Zugriffe werden ausschließlich über ADSC gesteuert (es gibt 2 ADSC-Signale, wobei jedes ein 32-Bit-Wort betrifft)). In der Betriebsart NX SRAM Connectivity ist hingegen ADSP an den ADS-Ausgang des Prozessors angeschlossen.
4) Verbindung fehlt beim 82343LX. Der 82343NX hat zwei weitere Ausgänge. Bei LX-kompatiblen Betrieb wirken diese als Schaltkreisauswahlsignale CCS1, 0 (jedes betrifft ein 32-Bit-Wort), die mit den CS-Eingängen der Speicherschaltkreise verbunden sind. Bei aktivierter NX SRAM Connectivity wirkt ein Signal als Schaltkreisauswahl für alle 64 bzw. 72 Bits (CCS1). Dann gibt es auch nur ein Signal für den Adreßvorschub (CADV0). Der Zweck: der NX kann durch Deaktivieren der CS-Eingänge die Stromaufnahme der Speicher vermindern (Power-Down-Modus). Es sind aber insgesamt nur 2 Anschlüsse des Steuerschaltkreises hierfür vorgesehen. (Beim LX wirken sie, wenn asynchrone RAMs angeschlossen sind, als CADV1, 0 bzw. beim NX als CCS1, 0. Sind an den NX synchrone RAMs angeschlossen, so wirkt as erste Signal als CS und das zweite als ADV für das gesamte 64-Bit-Wort.)

Hinweise:

1. PCMC = PCI and Memory Controller.
2. Die Abbildungen zeigen Anordnungen mit Paritätsbits. Viele Cache-Moduln speichern aber nur die 64 Datenbits.
3. Zur Cache-Konfiguration: die Steuerschaltkreise unterstützen die Konfigurationen (1) kein Cache, (2) 256 kBytes, (3) 512 kBytes). Abbildungsvermögen: 256 MBytes (unabhängig von der Cache-Größe). Schreibverfahren: bei LX zwischen Write Back und Write Thru umsteuerbar, bei NX nur Write Back. Burst-RAMs werden in Byte-Write-Organisation betrieben.

Die Abbildungen 2.122, 2.123 veranschaulichen verschiedene Konfigurationen entsprechender Cache-Moduln (zur Anschlußbelegung vgl. Abbildung 3.39b).

Abbildung 3.90 Cache-Moduln mit asynchronen SRAMs (IDT). a) ohne, b) mit eingebautem Adreßregister (Address Latch; hier: FCT3373)

Erklärung:
Die Ausführung mit eingebautem Adreßregister (b) ermöglicht es, auf dem Motherboard Platz zu sparen. *Praxistip:* Nachsehen, ob das Motherboard ein Adreßregister hat (nach Schaltkreisen ‘373 oder ‘573 suchen und Adreßleitungen verfolgen (Durchgangsprüfung in stromlosen Zustand - sind die Adreßleitungen des Cache direkt mit den Adreßanschlüssen des Prozessors verbunden oder nicht?)).

Abbildung 3.91 Cache-Modul mit synchronen Burst-SRAMs (IDT). a) Blockschaltbild, b) Signal-Übersicht

Hinweise:

1. "Asynchrone" Moduln sind typischerweise mit 3,3-V-SRAMs bestückt, "synchrone" Moduln hingegen mit 5-V-BSRAMs. Demgemäß werden im Modul entweder die 3,3-V- oder die 5-V-Speisespannungsanschlüsse genutzt.
2. Zu den Erkennungssignalen siehe Tabelle 3.24.

Presence-Detect-Signale			Bedeutung
PD2[1)]	PD1[2)]	PD0[2)]	
NC	NC	NC	kein Modul installiert
NC	GND	NC	asynchron, 256 kBytes (mit oder ohne Adreßregister)
GND	GND	NC	Flow Thru Burst, 256 kBytes
GND	GND	GND	Flow Thru Burst, 512 kBytes

1), 2): siehe Erklärung im Text

Tabelle 3.24 Erkennungssignale (Presence Detect)

Erklärung:

1) PD2 codiert die Speicherbestückung: NC = asynchron; GND = Flow Thru Burst,
2) PD1, PD0 codieren die Speicherkapazität: GND, NC = 256 kBytes; GND, GND = 512 kBytes.

3.4.2.4. Beispiel 4: Cache-Moduln mit eingebautem Cache Controller

Es liegt nahe, die gesamte Cache-Hardware auf einem Modul zusammenzufassen (Leistungsoptimierung; Cache Controller und Speicher können genau aufeinander abgestimmt werden). Abbildung 3.49 veranschaulicht eine Typenreihe derartiger Moduln, die zum direkten Anschluß an den Prozessorbus vorgesehen sind. Sie beruhen auf dem Controllerschaltkreis (mit eingebautem TAG-RAM) IDT71V280 (vgl. Abbildung 3.30).

Abbildung 3.92 Cache-Moduln mit eingebautem Cache Controller. a) mit asynchronen SRAMs, 256 kBytes, b) mit asynchronen SRAMs in 2 Banks (Interleaving-Betrieb), 512 kBytes, c) mit synchronen Pipelined-Burst-RAMs, 256 kBytes (IDT).

Hinweise:

1. Presence-Detect-Signale zum Codieren der Cache-Konfiguration sind nicht erforderlich, da Controller und Speicher jeweils eine feste Einheit bilden.
2. Zur Anschlußbelegung siehe Abbildung 3.39c.

3.4.2.5. Beispiel 5: Cache-Moduln gemäß COASt-Standard

Die COASt-Spezifikation wurde ursprünglich von Intel für den "Trident"-Schaltkreissatz (82430FX) ausgearbeitet (COASt = Cache on a Stick) und durch verschiedene Überarbeitungen für weiterentwickelte Schaltkreissätze (z. B. 82430HX und 82430VX) modifiziert. Sie ist zwischenzeitlich eine Art Industriestandard geworden. Tabelle 3.25 gibt einen Überblick über die Entwicklungsschritte. Die Abbildungen 3.50 bis 3.52 veranschaulichen verschiedene Ausführungsbeispiele.

Ausgabe des Standards	Inhalt
1.1	grundsätzliche Struktur, Anschlußbelegung
1.2	■ schärfere Forderungen an die Leiterplatten der Moduln: u. a. Leiterzüge mit 70 Ω Wellenwiderstand und Kontakte mit wenigstens 0,03 mil (0,7 Tausendstel mm) Goldauflage, ■ wählbare Burst-Adreßzählweise (Anschluß LBO bzw. BOSEL = Burst Order Select).
1.4	■ Serienwiderstände in den Datenleitungen (wahlweise), ■ 3,3-V-TAG-RAMs.
2.1	erweitertes Abbildungsvermögen (vgl. 82430HX)
3.0	diese Spezifikation faßt die Ausgaben 1.4 und 2.1 zusammen

Tabelle 3.25 Zur Entwicklung des COASt-Standards

Herkömmliche COASt-Moduln

Abbildung 3.50 zeigt ein Blockschaltbild, Tabelle 3.26 enthält die Belegungen der Erkennungssignale.

Abbildung 3.93 COASt-kompatibles Cache-Modul mit asynchronen SRAMs

Erklärung:
COASt bezieht sich stets auf Cache-Subsysteme, in denen wenigstens ein Teil der TAG-Speicherkapazität extern in asynchronen SRAMs bereitzustellen ist. Der Schaltkreissatz 82430FX erlaubt es, als Datenspeicher wahlweise asynchrone oder synchrone RAMs einzusetzen (vgl. Abschnitt 3.2.3.). Deshalb werden auch Moduln angeboten, die mit asynchronen SRAMs als Datenspeicher bestückt sind. Die Abbildung zeigt das Blockschaltbild eines solchen Moduls mit 256 kBytes Datenspeicher und 8k · 8-TAG-RAM. Das Modul ist mit einem Adreßregister (Address Latch) ausgerüstet (wird es nicht benötigt, ist CALE - vom Motherboard aus - fest mit High zu beschalten; das Latch-Register wirkt dann einfach als Puffer für die Adreßsignale - vgl. Abbildung 3.11).

Hinweise:

1. Die Steuersignalanschlüsse sind in der Abbildung angegeben, die Anschlußbelegung der Daten- und Adreßsignale sowie der Versorgungsspannungen entspricht dem allgemeinen COASt-Pinout (vgl. Abbildung 3.39c).
2. Derartige Moduln haben 5 Presence-Detect-Anschlüsse (Tabelle 3.26).
3. Erkennung derartiger Moduln: (1) an der Bestückung mit beispielsweise 8 SRAMs 32k · 8, (2) an Schaltkreisen ‘373 oder ‘573 (Adress Latch; auch Durchgangsprüfung: haben die Adreßanschlüsse direkte Verbindung zu den SRAMs oder nicht?), (3) anhand der Erkennungssignale (Tabelle 3.26).

Presence-Detect-Signale					Bedeutung
PD4*)	PD3	PD2	PD1	PD0	
NC	NC	NC	NC	NC	kein Modul installiert
GND	NC	GND	GND	NC	asynchron, 256 kBytes
GND	NC	GND	NC	NC	Pipelined Burst, 256 kBytes

GND	GND	NC	GND	GND	Pipelined Burst, 512 kBytes

*): Pin 114; Signal ist bei Moduln ab COASt-Spezifikation 1.2 mit LBO# beschaltet (Abbildung 3.39d, e)

Tabelle 3.26 Erkennungssignale von "asynchronen" COASt-Moduln (Presence Detect). Nach: Paradigm

Moderne COASt-Moduln

Typische Merkmale moderner COASt-kompatibler Moduln:

- Speicherkapazitäten 256 oder 512 kBytes,
- TAG-RAMs 8 bzw. 11 Bits · 8k oder · 16k (Bestückungsbeispiele: 2 · 8k · 8, 2 · 8k · 8 + 1 · 16k · 4, 2 · 32k · 8),
- Bestückung mit Flow-Thru- oder Pipelined-Burst-RAMs (manche Schaltkreissätze - z. B. 82430HX - unterstützen ausschließlich PBSRAMs),
- Speisespannung Datenspeicher: stets 3,3 V,
- Speisespannung TAG-RAM: 5 V oder 3,3 V,
- Burst-Adreßzählweise: über Eingang BOSEL (LBO#) wählbar[1), 2)],
- Schreiborganisation: Byte Select,
- die Anschlüsse der Burst-RAMs sind praktisch 1:1 herausgeführt, so daß man sich die funktionelle Bedeutung der Signale (gemäß Abbildung 3.39c, d) aus den Wirkprinzipien der Schaltkreise und den Cache-Prinzipschaltungen erschließen kann (vgl. Abschnitt 3.2.7. sowie Kapitel 2).

1) typischerweise ist das Signal auf dem Modul mit einem Pull-up-Widerstand beschaltet (≙ interleaved-Zählweise, wenn vom Motherboard aus nicht belegt),
2) es gibt auch Moduln mit festgelegter linearer Zählweise (z. B. für Cyrix 6X86-Prozessoren).

Wir zeigen im folgenden 2 Beispiele (Abbildungen 3.51, 3.52) sowie die Belegungen der Erkennungssignale (Tabelle 3.27).

Abbildung 3.94 COASt-kompatible Cache-Moduln (Corsair Microsystems). a) 256, b) 512 kBytes

Erklärung:
Es handelt sich um Moduln mit "normalem" Abbildungsvermögen (64 MBytes Cacheability). Sie sind mit 8 Bits breiten TAG-RAMs bestückt (bei 256 kBytes: 8k · 8, bei 512 kBytes: 16k · 8, wobei zumeist ein Schaltkreis 32k · 8 eingesetzt wird). Die Anordnung der Serienwiderstände ist nur sinnbildlich dargestellt (tatsächlich ist jeweils ein Widerstand - hier: 22 Ω (andere Anbieter verwenden z. B. 10 Ω) - in jede der 64 Datenleitungen geschaltet).

1) in 256-kBytes-Moduln sind #ECS1 und #ECS2 miteinander verbunden (1 Eingang, 1 Ausgang). ECS# wirkt als Schaltkreis-Auswahlsignal (Chip Enable). In 512-kBytes-Moduln sind die Anschlüsse nicht belegt (NC).
2) CLK0 ist das Taktsignal der ersten 256 kBytes,
3) CLK1 ist das Taktsignal der zweiten 256 kBytes. Beide Takte müssen synchron erregt werden (Grund für die getrennte Zuführung: Verringerung der kapazitiven Belastung des einzelnen Taktsignals).

Abbildung 3.95 COASt-3.0-kompatible Cache-Moduln (Cypress)

Erklärung:
Die Abbildung zeigt die "Architektur" derartiger Moduln. Je nach Speicherkapazität und Abbildungsvermögen ergeben sich verschiedene Bestückungs- und Anschlußvarianten.

1) erweiterter TAG-RAM (3 zusätzliche TAG-Bits zur Erweiterung des Abbildungsvermögens auf 512 MBytes). Typische Bestückung: 16k · 4 (wovon bei 256 kBytes nur 8k benötigt werden) oder 8k · 8 bzw. 32k · 8.
2) Adreßsignale: bei 256 kBytes A17...5, bei 512 kBytes A18...6,
3) bei 256 kBytes: mit Anschluß /ECS1 verbunden, bei 512 kBytes: mit Low (GND) verbunden (= ständig aktiv),
4) bei 256 kBytes: mit Anschluß /ECS1 verbunden ("Durchgang", bei 512 kBytes: nicht belegt (NC),
5) bei 256 kBytes mit Anschluß /ECS1, bei 512 kBytes mit Adreßsignal A18 verbunden,
6) Datenspeichererweiterung auf 512 kBytes.

Hinweis:
Zur Erweiterung des Abbildungsvermögens dienende TAG-Adressen sind, wenn nicht genutzt, typischerweise mit Pull-up-Widerständen beschaltet. TIO_{10} hat je nach Ausführung des Moduls keine Beschaltung oder einen Pull-up- oder einem Pull-down-Widerstand (je nach Ausführung des Moduls: erweitertes Abbildungsvermögen - kein erweitertes Abbildungsvermögen - DRAM-Cache).

Zu den Anschlüssen /ECS1, /ECS2
Diese sind nur in 256-kBytes-Moduln vorgesehen und dienen zur Modulauswahl in Konfigurationen aus einem fest eingebautem L2-Cache von ebenfalls 256 kBytes und einem Modul (vgl. Abbildung 3.3a). Motherboards, die keinen fest eingebauten Cache haben (vgl. Abbildung 3.3b), sollten /ECS1 mit Low belegen.

Erkennungssignale

Es sind 4 Erkennungssignale (Presence Detect PD3...0) vorgesehen (Zu den Anschlüssen vgl. Abbildung 3.39d). Es gibt allerdings keine durchgehend einheitliche Belegung. Tabelle 3.27 enthält eine Auswahl. (Vgl. auch Tabelle 3.26. Man beachte, daß hier PD4 fehlt (Pin 114 = LBO# (BOSEL)).)

Presence-Detect-Signale				Bedeutung
PD3[1)]	PD2[1)]	PD1[2)]	PD0[2)]	
NC	NC	NC	NC	kein Modul installiert
NC	GND	NC	NC	256 kBytes[1)], auch: erweitertes Abbildungsvermögen
GND	NC	GND	GND	512 kBytes[2)], auch: erweitertes Abbildungsvermögen
NC	GND	GND	NC	256 kBytes[3)]
GND	NC	GND	NC	512 kBytes[3)]
GND	GND	NC	NC	512 kBytes, DRAM-Cache[4)]

1) bis 4): siehe Erklärung im Text

Tabelle 3.27 Erkennungssignale (Presence Detect). Auswahl nach diversen Datenblättern

Erklärung:

1) industrie-üblich für 256 kBytes,
2) industrie-üblich für 512 kBytes,
3) gelegentlich für Moduln mit normalem Abbildungsvermögen (· 8-TAG-RAMs) verwendet, wenn gemäß 1) und 2) Moduln mit erweitertem Abbildungsvermögen (Extended Cacheability für 82430HX) gekennzeichnet werden,

4) Kennzeichnungsbeispiel; IDT Fusion Memory.

Bestellbezeichnungen
Abbildung 3.53 veranschaulicht anhand einer typischen Bestellbezeichnung, worauf zu achten ist.

Abbildung 3.96 Beispiel einer Bestellbezeichnung (nach: Corsair Microsystems)

Erklärung:

a) Speichergröße. NNNX = “256k” oder = “512k”,

b) COASt-Kompatibilität. NXN nicht vorhanden (Leerzeichen): nur Anschlußbelegung COASt-kompatibel, NXN = “2x1" ≙ kompatibel zu COASt 2.1, NXN = “3.x” ≙ kompatibel zu COASt 3.0, NXN = “6X86" ≙ lineare Adreßzählweise.

Das Beispiel läßt allerdings nicht alle Wahlmöglichkeiten erkennen (hierzu gehören: Taktfrequenz, erweitertes Abbildungsvermögen (Extended Cacheability) sowie die Deselect-Organisation (DCD, SCD; vgl. Abschnitt 3.3.). Im Fall des Falles immer im aktuellen Datenmaterial der Anbieter nachsehen.

3.5. Entwicklungstendenzen

Die wichtigste Anforderung an L2-Caches ist, daß sie mit dem jeweiligen Prozessor Schritt halten. Idealforderung: bei jeder beliebigen Frequenz des Prozessor-Bustaktes alle Anforderungen (sofern sie Treffer sind) ohne Wartezustände zu bedienen. Eine übermäßige Vergrößerung des Cache ist demgegenüber weniger sinnvoll (typische - und beim Stand der Technik zweckmäßige - Cache-Größen liegen zwischen 256 kBytes und 1 MBytes. Weitere Anforderungen betreffen die Trefferrate, die Gewährleistung der Cache-Kohärenz in Multiprozessorkonfigurationen und die Betriebszuverlässigkeit.

Diese Forderung versucht man mit folgenden Ansätzen zu erfüllen:

- Verbesserung der Schaltungsintegration (Extremfall: der gesamte L2-Cache auf einem Schaltkreis),
- direktes Zusammenwirken zwischen Cache und Prozessor über spezielle Bussysteme (Beispiel: Dual Independent Bus Architecture (Intel)),
- Implementierung 2- oder 4-fach assoziativer Abbildungsprinzipien,
- Erweiterung des Abbildungsvermögens auf den gesamten linearen Adreßraum,
- flexiblere programmseitige Steuerbarkeit der Cache-Umgehung bzw. der Aufteilung des Adreßraumes (in “cacheable” und “non-cacheable” Bereiche),
- Verwirklichung von TAG-RAM-Strukturen mit mehreren Zustandsbits; Implementierung höher entwickelter Kohärenz-Protokolle (wie z. B. MESI) auch im L2-Cache,
- Implementierung von Paritätskontrolle oder Fehlerkorrektur (ECC) auch im L2-Cache (Beispiele: Pentium Pro und Pentium II).

Online-Informationsquellen (Auswahl)

http://www.corsairmicro.com
http://www.cypress.com (Schaltkreissätze, Speicher und Cache-Moduln)
http://www.idt.com
http://www.intel.com, nähere technische Informationen: http://developer.intel.com
http://www.micron.com
http://www.mosys.com (synchrone MCache-Schaltkreise)
http://www.mot.com (Motorola), nähere technische Informationen: http://design-net.com
http://www.opti.com (Schaltkreissätze)
http://www.smartm.com (SMART Modular Technologies)

http://www.prdm.com (Paradigm)