

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3848965号
(P3848965)

(45) 発行日 平成18年11月22日(2006.11.22)

(24) 登録日 平成18年9月1日(2006.9.1)

(51) Int. Cl.

G06F 9/30 (2006.01)

F I

G06F 9/30 330Z

請求項の数 24 (全 17 頁)

(21) 出願番号	特願2005-502328 (P2005-502328)	(73) 特許権者	594154428
(86) (22) 出願日	平成15年10月6日(2003.10.6)		エイアールエム リミテッド
(65) 公表番号	特表2006-510127 (P2006-510127A)		イギリス国 シービー1 9エヌジェイ
(43) 公表日	平成18年3月23日(2006.3.23)		ケンブリッジ, チェリー ヒントン, フル
(86) 国際出願番号	PCT/GB2003/004304		バーン ロード 110
(87) 国際公開番号	W02004/053685	(74) 代理人	100066692
(87) 国際公開日	平成16年6月24日(2004.6.24)		弁理士 浅村 皓
審査請求日	平成17年11月4日(2005.11.4)	(74) 代理人	100072040
(31) 優先権主張番号	0229068.2		弁理士 浅村 肇
(32) 優先日	平成14年12月12日(2002.12.12)	(74) 代理人	100094673
(33) 優先権主張国	英国 (GB)		弁理士 林 拓三
(31) 優先権主張番号	0302650.7	(74) 代理人	100091339
(32) 優先日	平成15年2月5日(2003.2.5)		弁理士 清水 邦明
(33) 優先権主張国	英国 (GB)		

最終頁に続く

(54) 【発明の名称】 データ処理装置内の命令タイミング制御

(57) 【特許請求の範囲】

【請求項1】

データ処理装置であって、

終了するまでに最小のサイクル数と最大のサイクル数との間のサイクル数を必要とする少なくとも1つの可変タイミング命令を含む複数の異なるプログラム命令に応じて、終了するまでに多くの処理サイクルをそれぞれ必要とする個別の処理動作を実行するプロセッサを備え、

前記プロセッサは可変タイミング・モードで動作して、前記少なくとも1つの可変タイミング命令は終了するまでに可変の処理サイクル数をかけることが許され、また、

前記プロセッサは固定タイミング・モードで動作して、前記少なくとも1つの可変タイミング命令は終了するまでに前記最大のサイクル数をかけることを強制される、
データ処理装置。

【請求項2】

前記少なくとも1つの可変タイミング命令は条件付き命令を含み、前記プロセッサは前記可変タイミング・モードで動作して1つ以上の前に実行したプログラム命令の実行に応じて1つ以上の条件コード集合に従って前記条件付き命令の実行を抑制し、また前記プロセッサは前記固定タイミング・モードで動作して1つ以上の前に実行したプログラム命令の実行に応じて前記1つ以上の条件コード集合に関係なく固定の処理サイクル数で前記条件付き命令を終了する、請求項1記載のデータ処理装置。

【請求項3】

前記条件付き命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付き命令の実行を抑制する場合は、前記条件付き命令は後のデータ処理動作に影響を与える何らかの変更を行うことが禁じられる、請求項 2 記載のデータ処理装置。

【請求項 4】

前記条件付き命令が条件付き分岐命令である場合は、前記条件付き分岐命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付き分岐命令の実行を抑制する場合は、前記条件付き分岐命令内で指定されている分岐先に関係なく、前記条件付き分岐命令は次の命令に分岐することを強制される、請求項 3 記載のデータ処理装置。

10

【請求項 5】

前記条件付き命令が条件付きデータ操作命令である場合は、前記条件付きデータ操作命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付きデータ操作命令の実行を抑制する場合には、前記条件付きデータ操作命令は前記条件付きデータ操作命令のどの通常の結果宛先にも結果を書き込むことが禁じられる、請求項 3 記載のデータ処理装置。

【請求項 6】

どの通常の結果宛先にも前記結果を書き込むことが禁じられる場合は、代わりに前記結果は少なくとも 1 つのダミー宛先に書き込まれる、請求項 5 記載のデータ処理装置。

【請求項 7】

20

前記少なくとも 1 つのダミー宛先はダミー・プロセッサ・レジスタを含む、請求項 6 記載のデータ処理装置。

【請求項 8】

前記少なくとも 1 つの可変タイミング命令は処理中の 1 つ以上のデータ値に従って早期終了を行うことが可能な命令を含み、また前記プロセッサは前記可変タイミング・モードで動作するときは早期終了が許され、前記プロセッサは前記固定タイミング・モードで動作するときは早期終了が禁じられる、請求項 1 記載のデータ処理装置。

【請求項 9】

早期終了が可能な前記命令は、
多重サイクル乗算命令と、
多重サイクル除算命令と、
多重サイクル加算命令と、
多重サイクル減算命令と

30

の 1 つである、請求項 8 記載のデータ処理装置。

【請求項 10】

前記プロセッサは、プログラマブル・モード制御用パラメータに従って前記可変タイミング・モードか前記固定タイミング・モードを採用する、先行請求項のどれかに記載のデータ処理装置。

【請求項 11】

前記プログラマブル・モード制御用パラメータはシステム構成レジスタ内に記憶される、請求項 10 記載のデータ処理装置。

40

【請求項 12】

前記プロセッサはプログラム実行経路を隠すために前記固定タイミング・モードに切り替えられる、先行請求項のどれかに記載のデータ処理装置。

【請求項 13】

終了するまでに最小のサイクル数と最大のサイクル数との間のサイクル数を必要とする少なくとも 1 つの可変タイミング命令を含む複数の異なるプログラム命令に応じて、終了するまでに多くの処理サイクル数をそれぞれ必要とする個別の処理動作を実行するプロセッサを用いてデータを処理する方法であって、

前記プロセッサを可変タイミング・モードで動作させて、前記少なくとも 1 つの可変タ

50

イミング命令は終了するまでに可変の処理サイクル数をかけることが許され、

前記プロセッサを固定タイミング・モードで動作させて、前記少なくとも1つの可変タイミング命令は終了するまでに前記最大のサイクル数をかけることを強制される、ステップを含むデータを処理する方法。

【請求項14】

前記少なくとも1つの可変タイミング命令は条件付き命令を含み、また更に前記プロセッサを前記可変タイミング・モードで動作させるときは1つ以上の前に実行したプログラム命令の実行に応じて1つ以上の条件コード集合に従って前記条件付き命令の実行を抑制し、また前記プロセッサを前記固定タイミング・モードで動作させるときは1つ以上の前に実行したプログラム命令の実行に応じて前記1つ以上の条件コード集合に関係なく固定の処理サイクル数で前記条件付き命令を終了することを含む、請求項13記載のデータを処理する方法。

10

【請求項15】

前記条件付き命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付き命令の実行を抑制する場合には、前記条件付き命令は後のデータ処理動作に影響を与える何らかの変更を行うことが禁じられる、請求項14記載のデータを処理する方法。

【請求項16】

前記条件付き命令が条件付き分岐命令である場合は、前記条件付き分岐命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付き分岐命令の実行を抑制する場合は、前記条件付き分岐命令内で指定されている分岐先に関係なく、前記条件付き分岐命令は次の命令に分岐することを強制される、請求項15記載のデータを処理する方法。

20

【請求項17】

前記条件付き命令が条件付きデータ操作命令である場合は、前記条件付きデータ操作命令を前記固定タイミング・モードで実行するとき、前記条件付きコードが前記可変タイミング・モードでは前記条件付きデータ操作命令の実行を抑制する場合は、前記条件付きデータ操作命令は前記条件付きデータ操作命令のどの通常の結果宛先にも結果を書き込むことが禁じられる、請求項15記載のデータを処理する方法。

【請求項18】

どの通常の結果宛先にも前記結果を書き込むことが禁じられる場合は、代わりに前記結果は少なくとも1つのダミー宛先に書き込まれる、請求項17記載のデータを処理する方法。

30

【請求項19】

前記少なくとも1つのダミー宛先はダミー・プロセッサ・レジスタを含む、請求項18記載のデータを処理する方法。

【請求項20】

前記少なくとも1つの可変タイミング命令は処理中の1つ以上のデータ値に従って早期終了を行うことが可能な命令を含み、また更に前記プロセッサは前記可変タイミング・モードで動作するときには早期終了が許され、前記プロセッサは前記固定タイミング・モードで動作するときには早期終了が禁じられることを含む、請求項13記載のデータを処理する方法。

40

【請求項21】

早期終了が可能な前記命令は、
多重サイクル乗算命令と、
多重サイクル除算命令と、
多重サイクル加算命令と、
多重サイクル減算命令と
の1つである、請求項20記載のデータを処理する方法。

【請求項22】

前記プロセッサは、プログラマブル・モード制御用パラメータに従って前記可変タイミ

50

ング・モードか前記固定タイミング・モードを採用する、請求項 1 3 から 2 1 のどれかに記載のデータを処理する方法。

【請求項 2 3】

前記プログラマブル・モード制御用パラメータはシステム構成レジスタ内に記憶される、請求項 2 2 記載のデータを処理する方法。

【請求項 2 4】

前記プロセッサはプログラム実行経路を隠すために前記固定タイミング・モードに切り替えられる、請求項 1 3 から 2 3 のどれかに記載のデータを処理する方法。

【発明の詳細な説明】

【技術分野】

10

【0 0 0 1】

本発明はデータ処理装置の分野に関するものである。より特定すると、本発明は少なくとも複数のプログラム命令が終了するまでに可変の処理サイクル数を必要とするデータ処理装置に関するものである。

【背景技術】

【0 0 0 2】

終了するまでに可変の処理サイクル数を必要とする命令を有するプロセッサ・コア（例えば、英国キャンブリッジのARM社の設計によるもの）が提供されている。このようなプログラム命令の一例は条件付命令である。これは、先行命令を実行した結果或る条件が満足される場合（例えば、先行命令により結果がゼロ、オーバーフロー、桁上げなどになった場合）にだけ実行されるよう符号化される。プロセッサの性能を高めるため、早期終了方式を備えるプロセッサも提供されている。これは、処理サイクルを続けても結果が変わらないとプロセッサが判定した場合は、マルチサイクル演算を早期に終了するものである。例えばマルチサイクル加算演算において、両方のオペランドの高次のビットが全てゼロであれば、桁上げがないと判定された場合はその後のプロセッサ・サイクルで高次のビットを計算する必要がない。終了するまでに可変の処理サイクル数をかけるプログラム命令は他にも例が多い。

20

【0 0 0 3】

例えば高度の機密保護で動作して、処理中のデータに許可なくアクセスすることが出来ないようにするプロセッサを提供することがますます重要になっている。例えば、金融取引を扱うスマートカードに用いられるプロセッサ・コアは、パスワードやデータなどを証明するために高度に秘密の暗号鍵を用いることが多い。装置の機密保護と完全性を保持するには、このような暗号鍵は秘密にしなければならない。このような装置の機密保護を攻撃する 1 つの周知の方法は、所定の動作を終了するまでに要する処理サイクル数を数えて、処置中のデータに関する情報を識別しようと試みることである。要した処理サイクル数と処理中のデータとの間に相関がある場合は、処理中のデータに関する情報を知ることができる。

30

【発明の開示】

【発明が解決しようとする課題】

【0 0 0 4】

40

サイクルを数えることにより装置の機密保護に加えられる攻撃を防ぐための周知の方法は、コンピュータ・プログラム・コードの書き方に注意して、コンピュータ・プログラムのフローに無関係に固定のサイクル数で終了させることである。実際には、これを行うのは困難である。なぜなら、高いレベルの知識と熟練がプログラマに要求されるためと、全ての場合に処理サイクル数を等しくするという所望の目的が達成されたことを確認／テストすることが困難なためである。また、プログラマが普通に用いる生産性向上ツール（コンパイラなど）はこのような機密のコードを生成するのに適していない。なぜなら、通るプログラム経路に従って、このようなツールが作るコードは処理サイクル数が大幅に変わるのが普通だからである。

【課題を解決するための手段】

50

【0005】

1つの観点から、本発明が提供するデータ処理装置は、

終了するまでに最小のサイクル数と最大のサイクル数との間のサイクル数を必要とする少なくとも1つの可変タイミング命令を含む複数の異なるプログラム命令に応じて、終了するまでに多くの処理サイクルをそれぞれ必要とする個別の処理動作を実行するプロセッサを備え、

前記プロセッサは可変タイミング・モードで動作して、前記少なくとも1つの可変タイミング命令は終了するまでに可変の処理サイクル数をかけることが許され、また、

前記プロセッサは固定タイミング・モードで動作して、前記少なくとも1つの可変タイミング命令は終了するまでに前記最大のサイクル数をかけることを強制される。

10

【0006】

本発明の認識では、処理動作を速くしまた電力消費を減らすためにプロセッサ内で用いられる可変タイミング命令は、要した処理サイクル数と処理中のデータとの関係を完全に隠すことが望ましい安全な装置という文脈では明らかに不利である。同時に、機密のデータを処理していないときは、速度を上げたり電力消費を減らしたりする可変タイミング命令に付随する大きな利点は望ましいものである。本発明は上記の問題を認めると共に、可変タイミング・モードと固定タイミング・モードとで動作する装置を提供することにより、可能な環境で現在の装置に付随する利点を保持する。可変タイミング・モードでは、可変タイミング命令は終了するまでに可変の処理サイクル数をかけることが許され、固定タイミング・モードでは、可変タイミング命令は終了するまでに必ず固定のサイクル数をかけるよう強制される。このように、機密のデータを処理するときは装置を固定タイミング・モードに置いて、処理動作を終了するまでにかかる処理サイクル数を容易に隠すが、機密のデータを処理しないときは装置を可変タイミング・モードで動作させて、可変タイミングの機構に付随する速度の利点と電力消費削減の利点とを活用する。固定タイミング・モードを用いると各命令のタイミングは処理中のデータとは無関係なので、プログラム・フローの経路に無関係に、プログラマは終了するまでに固定の処理サイクル数をかけるプログラム・コードを書くのが容易になる。またこれにより、固定タイミング・コードを生成するコンパイラを作るのが容易になる。

20

【0007】

前に述べたように、本発明の方法は可変タイミングをとることのできる広範囲のプログラム命令に適用可能であるが、特に適しているのは、装置が固定タイミング・モードにあって全ての条件コードに関係なく条件付き命令は固定の処理サイクル数をかけることを強制される場合か、可変タイミング・モードにあって条件コードが或るパラメータと一致する場合は命令の実行が抑制される場合かに従って、1つ以上の条件付き命令が実行される実施の形態である。

30

【0008】

可変タイミング・モードでは抑制すべき条件付き命令を固定タイミング・モードで実行する場合は、本発明の好ましい実施の形態では、後のデータ処理に影響を与えるような変更を条件付き命令が行うことは全て禁止される。例えば、後の処理に影響するようなプロセッサ内の状態の更新や変更を条件付き命令が行うことは全て禁止される。

40

【0009】

本発明の技術が適しているプログラム命令の種類は条件付き分岐命令である。なぜなら、この技術を用いなければ、分岐が抑制されるかどうかに従ってこの種の命令はプログラム・タイミングに強い影響を与えることがあるからである。固定タイミング・モードで動作するとき、条件付き分岐命令は条件コードが満足されない場合でも分岐することを強制されるが、この場合は条件付き分岐命令に指定された分岐先に関係なくプログラム・フロー内の次の命令に分岐され、条件付き分岐命令が全く抑制された場合と同じように次の命令が実行される。

【0010】

条件付き命令が条件付きデータ操作命令の場合は、本発明の好ましい実施の形態では、

50

固定タイミング・モードにあるときは、条件コードを失敗したときは条件付きデータ操作命令は実行されるが、通常これは抑制されて、命令は実行されるが条件付きデータ操作命令の通常の結果の宛先に結果を書き込むことは禁止される。

【0011】

条件付きデータ操作命令から結果が書き込まれるかどうかに従って生じるプロセッサの消費電力の変動を観察してこれに基づいて機密保護に対する攻撃が行われることから守るために、好ましい実施の形態では、条件コードを失敗したときに、結果を通常の結果の宛先に書き込むのではなく1つ以上のダミー宛先に書き込む。これにより、条件コードを失敗したかどうかに関係なく実質的に同じ電力消費が保たれ、条件付きデータ操作命令は必ず実行され、ダミーの宛先ではあるにしても結果は必ず書き込まれる。

10

【0012】

可変タイミング実行が可能な命令の別の型は、1つ以上の処理中のデータ値に従って早期終了が可能な命令である。好ましい実施の形態は固定タイミング・モードで動作して、このような早期終了可変タイミング・モードを与えるために装置内に設けられた機構がそれが可能であることを示しているときでも、早期終了を全て抑制する。例えば、乗算の一方のオペランドがゼロであれば他方のオペランドが何であっても結果はゼロなので、結果をゼロとして命令を早期に終了させることができる。しかし固定タイミング・モードでは、命令は処理サイクル数を全てかけてゼロの結果を返すよう強制される。

【0013】

早期終了が可能な好ましい型の命令の例として、マルチサイクル乗算命令、マルチサイ

20

クル除算命令、マルチサイクル加算命令、マルチサイクル減算命令がある。
或るハードウェア信号などによって装置を固定タイミング・モードにすることは可能であるが、本発明の好ましい実施の形態では、プログラマブル・モード制御用パラメータ（例えば、1ビットまたは複数のビット）によって可変タイミング・モードか固定タイミング・モードかを採用するようプロセッサを構成してよい。

【0014】

このようにして、機密のデータを処理中でなくかつ低い電力消費で高い性能が必要なときは可変タイミング・モードにし、機密のデータを処理中であって処理中のデータが処理サイクル数に依存することを隠す必要性の方が速度や電力消費などの考慮より優先するときは固定タイミング・モードにするというように、ソフトウェア制御の下で装置を切替

30

えることができる。
プログラマブル・モード制御用パラメータを設定する好ましい方法は、装置制御用コプロセッサなどのシステム構成レジスタ内にこれを保存することである。

【0015】

別の形態から見ると、本発明は終了するまでに最小のサイクル数と最大のサイクルの数との間を必要とする少なくとも1つの可変タイミング命令を含む複数の異なるプログラム命令に応じて、終了するまでに多くの処理サイクル数をそれぞれ必要とする個別の処理動作を実行するプロセッサを用いてデータを処理する方法を提供し、前記方法は、

前記プロセッサを可変タイミング・モードで動作させて、前記少なくとも1つの可変タイミング命令は終了するまでに可変の処理サイクル数をかけることが許され、

40

前記プロセッサを固定タイミング・モードで動作させて、前記少なくとも1つの可変タイミング命令は終了するまでに前記最大のサイクル数をかけることを強制される、ステップを含む。

【実施例】

【0016】

図1は、プロセッサ・コア4と、コプロセッサ6と、メモリ8とを含むデータ処理装置2を示す。

動作を説明すると、プロセッサ・コア4はメモリ8から命令とデータとを取り出す。命令は命令パイプライン10に取り出され、例えば、取出し、復号、実行、メモリ、次の処理サイクルでの書き込みなど順次のパイプライン段を占める。パイプライン付きプロセッ

50

サ自体は、部分的に重ねることにより多数のプログラム命令を実質的に実行してプロセッサの性能を向上させる方法として周知である。

【0017】

プロセッサ・コア4がメモリ8から読み取ったデータ値はレジスタ・バンク12に送られ、ここから乗算器14、シフタ16、加算器18の1つ以上を用いてプログラム命令制御の下に操作される。AND、OR、ゼロまでのカウントなどの論理演算を実行する回路などの他のデータ操作回路も設けられる。

【0018】

図1はプロセッサ・コア4内の命令復号器20も示す。これは命令パイプライン10内のプログラム命令に応じて実行制御信号を生成して、レジスタ・バンク12、乗算器14、シフタ16、加算器18などの種々の処理要素に与えて、実行される処理動作を制御する。例えば、復号器20が生成する制御信号は該当するオペランドをレジスタ・バンク12から読み取り、乗算器14、シフタ16、加算器18の該当する要素に与えて実行して結果を生成し、これをレジスタ・バンク12に戻して書き込む。

10

【0019】

コプロセッサ6は多数の構成レジスタ22を含むシステム構成コプロセッサである。構成レジスタ22はプログラム制御の下に書き込まれて構成制御用パラメータを設定する。このような構成制御用パラメータは処理装置2の構成の多くの形態（例えばエンディアネス（endianness）など）を指定する。このような構成制御用レジスタ22の1つの中に、プロセッサ・コアの動作を固定タイミング・モードで行うか可変タイミング・モードで行うかを指定する1つのビットが含まれる。図ではこのビットは命令復号器20の入力として与えられるように示しているが、認識されるように、このビットはその行動を制御する必要に応じてプロセッサ・コア4内の種々の他の点に与えてもよい。この固定／可変ビットに従って、プロセッサ・コア4は固定タイミング・モードまたは可変タイミング・モードで動作する。

20

【0020】

固定タイミング・モードでは、可変タイミング・モードで可変タイミング（すなわち、終了するまでに可変の処理サイクル数をかける）を有する少なくとも1つのプログラム命令は、可変ではなく固定タイミングを有するように強制される（例えば、全体として抑制されたかまたは最大の処理サイクル数より早く終了したかに関わらず、終了するまでに最大の可能な処理サイクル数をかける）。命令復号器20は、プログラム命令を復号してプロセッサ・コア4の他の要素の活動を命令する主役なので、命令復号器20はプロセッサ・コア4の動作を固定タイミング・モードか可変タイミング・モードかに制御するのに主導的な役割を果たす。全ての可変タイミング命令が固定タイミング・モード型の動作を行う必要はない。

30

【0021】

認識されるように、上の説明では構成制御用レジスタ22内の1つのビットでタイミング・モードを固定か可変かに切替えるものとして示した。他の方法として、構成制御用レジスタ22内の複数のビットを用いて、異なる型の命令（条件付き命令行動、均一分岐行動、早期終了の禁止など）の固定または可変のタイミング行動を別々に可能にしたり禁止にしたりよい。

40

【0022】

図2は条件付き命令24の概要を示す。この条件付き命令は、複数の条件付き命令だけを含む命令集合の一部でもよいし、実質的に完全に条件付きである命令集合（ARM命令集合など）の一部でもよい。条件コード26は、関連する命令を実行するかしないかという一組のプロセッサ状態条件を符号化する。例えば条件コード26は、装置内に現在設定されている条件コードがゼロの結果や、桁上げの発生や、オーバーフローの発生などを示す場合は命令24を実行しないと指定することができる。この型の命令を用いて効率的なプログラム符号化を行うことができる。固定／可変ビットは条件付き行動を少なくとも部分的に抑制する。すなわち、その条件コードに関係なく命令は実行するが、プロセッサ状

50

態に影響を与えるようなその結果の書き込み方はしない。

【0023】

図3は命令復号器20が実行する処理動作の一部の概要を示す流れ図である。理解されるように、図3はこのような処理動作を論理シーケンスとして示すが、実際にはこのような処理動作は少なくとも部分的に並列にまたは異なる順序で実行してよい。

【0024】

ステップ28で、命令復号器20は実行する新しい命令を待つ。新しい命令を受けると、処理はステップ30に進み、新しい命令に関連する条件コードを読み取る。ステップ32で、これらの条件コードと装置内の既存の条件コードとを比較する。装置内のこれらの既存の条件コードは、前の処理活動（直前の命令かまたはこれらの条件コードを更新した最新の命令で行った）の結果である。

10

【0025】

ステップ34で、実行される現在の命令の条件コード26と既存の条件コードとが一致するかどうかチェックする。一致しない場合は、処理はステップ36に進み、現在の命令の実行を開始する。認識されるように、図3は一致しない場合に実行する装置を示すが、別の実施の形態では一致する場合に実行する装置でもよい。

【0026】

ステップ36の後、処理はステップ38に進んで、命令の早期終了が可能かどうかチェックする。この早期終了は、例えば、オペランドの1つが特定の値（0や1など）を有するためか、または次の処理サイクルで特定の部分的結果が作られたためである。早期終了が可能な場合は処理はステップ40に進み、プロセッサ・コア4が現在動作中のタイミング・モードが固定か可変かをチェックする。プロセッサが可変タイミング・モードにある場合は処理はステップ42に進み、関係する命令を早期終了し、結果を適当に返して、処理はステップ28に戻る。

20

【0027】

ステップ40で装置が固定タイミング・モードにあると判定された場合は、早期終了が可能であるかどうかに関係なく処理はステップ44に進む。ステップ38で早期終了が可能でないと判定されたときにもステップ44に進むが、関係する命令をここで1処理サイクルの間実行する。乗算や除算や加算や減算などのマルチサイクル処理命令の場合は実行するのに一般に数サイクルを要するので、ステップ44の後で処理はステップ46に進み、その命令に関連する最大のサイクル数を実行したかどうか判定する。最大のサイクル数を実行した場合は結果が生成されている。早期終了が可能ではあるが更に続いて複数の処理サイクル間実行するよう装置が強制された場合も、その型の命令の最大の可能な処理サイクル数に到達したときはこの強制実行を終了してよいことをステップ46は示す。最大の処理サイクル数をまだ実行していない場合は、処理はステップ38に戻る。

30

【0028】

ステップ34でのテストで一致した場合は、処理はステップ48に進む。この例では、ステップ34で一致したと検出されたことは、特定の命令の実行を抑制すべきことを示す。ステップ48で、装置が現在強制実行モードにあるかどうか判定する。強制実行モードにある場合は処理はステップ50に進み、命令の強制ダミー実行を行う。ダミー実行を行ったときは、命令自体の中に指定されている宛先ではなくトラッシュ・レジスタ（図1のトラッシュ・レジスタ51を参照）に結果を書き込んで、抑制すべきであったので実行してはならなかったプログラム命令によって装置の状態が変更されるのを防ぐと共に、電力消費を実質的に不変に保つ。ステップ48で装置が強制実行モードではなく可変タイミング・モードにあると判定された場合は、処理はステップ50をバイパスしてステップ28に戻り、プログラム命令は通常の方法で抑制される。

40

【0029】

認識されるように、図3は条件コードを失敗した全ての命令と命令の全ての早期終了を抑制したものにダミー実行が適用される一般的な装置を示す。実際には、このような方法は条件付き命令と早期終了が可能な命令の部分集合にも適用することができる。上に述べ

50

た複数の構成制御用ビットを用いて、早期終了抑制などの機能は選択的に実行するが、条件コードの失敗の後のダミー実行などの他の機能は実行しないようにすることもできる。

【0030】

図4は、固定タイミング・モードにおける条件付き分岐命令の実行の概要を示す。命令のシーケンスA Bを、条件付き分岐命令B E Q（等しいとき分岐）に到達するまで実行する。命令B E Qは、前の処理と結果が等しいことを示すフラグがセットされている場合は指定された分岐を実行し、このフラグがセットされていない場合は抑制するという行動を符号化する。条件コードが合格のとき（すなわち、条件コードが一致するとき）は分岐を行って、処理は命令X、Yなどに進む。条件コード失敗のときは、全体を抑制するのではなく、B E Q命令はすぐ次の命令Cに分岐する。これは、B E Q命令が抑制されて全く実行されなかった場合に到達する命令と同じである。しかし固定タイミング・モードでは、条件コードが合格か失敗かに関係なくB E Qは同じ処理サイクル数になる。これにより、秘密データにアクセスしようとする人に対して前に実行したデータ処理動作の結果を隠すことができる。

10

【0031】

図5は、プログラム命令Iに回答してデータDを操作するプログラマブル・プロセッサ・コアの形のデータ処理装置52の略図を示す。データ処理装置52は、レジスタ・バンク54、乗算器56、シフタ58、加算器60、算術論理ユニット62、ロード・ストア・ユニット64、データ・パイプライン66、命令復号器68、ランダム・クロック・ゲート用回路70を含む。システム構成コプロセッサC P 1 5 7 2はプロセッサ・コアに結合する。システム構成コプロセッサ72は、データ処理装置52の種々の回路部の擬似ランダム・ダミー活動をそれぞれ可能にしたりは使用禁止にする多数のフラグ値を保持するシステム構成レジスタ74を含む。認識されるように、データ処理装置52は一般に更に多くの回路要素を含むが、簡単のために図5では省略した。

20

【0032】

乗算器56に付随するのはダミー活動可能回路76である。これは必要に応じて乗算器56内でのダミー活動を可能にし、または実行中のプログラム命令が必要とするときは、必要な活動可能信号を通して乗算器56を活動的にする。同様なダミー活動可能回路78, 80, 82, 84が前に述べた他の各回路部58, 60, 62, 64に付随する。

【0033】

動作を説明すると、実行する命令は命令パイプライン66に、更に命令復号器68に送られて命令駆動可能信号を生成し、各回路部に与えられる。このような可能信号は、データ処理装置52を通るデータ経路を選択し、関係する回路部を活動的にしてその入力を読み取り、指定された処理を実行し、その関連する出力信号を生成する。例えば、乗算・累算演算はレジスタ・バンク54からデータ値を読み取り、これを乗算器56と加算器60とに与え、その結果をレジスタ・バンク54に返して書き込む。このように、レジスタ・バンク54と乗算器56と加算器60とは全てその動作を可能にしたりそれを選択する必要な活動可能信号を受けて、完全なデータ経路を形成する。

30

【0034】

異なる回路部は異なる電力消費特性とタイミング特性とを有するので、外部の観察者はこのようなパラメータを観察することによりどの命令を実行中かを知ることができる。これに対抗して、実行中の命令に必要な他の回路部の擬似ランダム・ダミー活動も可能にする。例えば、実行中の特定の乗算・累算命令でシフタ58が用いられていなくても、擬似ランダム的に可能にして、その入力に与えられる全ての値をシフトして電力を消費する。このダミー活動が必要な動作（例えば、或る回路部が出力値を持続する）を妨げるような望ましくない方法で回路状態を変えることを防ぐため、その出力ラッチは可能にしない。ダミー活動が可能になるのは、関係する回路部の通常の動作タイミングと一致する期間である。

40

【0035】

ランダム・クロック・ゲート用回路70は異なる各回路部向けの複数の擬似ランダム可

50

能信号を受けてこれをゲートし、システム構成コプロセッサ72内のシステム構成レジスタ74から読み取られた構成パラメータの制御の下に各回路部に与える。このような構成フラグは、例えば、シフタ58、ALU62、乗算器56についてはダミー活動を可能にするが、加算器60とロード・ストア・ユニット64については可能にしないことを示す。異なる擬似ランダム可能信号により、関係するこれらの各回路部と一致させて異なる擬似ランダム特性を与えることができる。例えば、異なる回路部の通常のタイミングに関連して異なる最小可能時間があってよい。

【0036】

全体レベルにおいて、命令復号器68は現在実行中の命令が指定するデータ処理動作を実行するのに必要な回路部を可能にする必要な活動可能回路として機能することが分かる。この必要な活動に重ねて、データ処理装置52の他の種々の場所に設けられているダミー活動制御回路により、他の回路部内の種々のダミー活動が可能になり／刺激される。ダミー活動は、必要な活動に付随する電力消費およびタイミング特性を隠すのに役立つ。

10

【0037】

図6は、必要な可能信号enとダミー可能信号rndとを受ける回路部86を示す略図である。この回路部86は、その間で処理論理がデータ値を操作するラッチのシーケンスと考えることができる。真に要求された活動が必要なとき、回路部86を通るデータ経路を与える全てのラッチが可能になり、要求された処理は入力ラッチと出力ラッチとの間で実行される。ダミー活動が命令されると、入力ラッチと中間ラッチだけが可能になる。この場合は、全回路部を通してデータ経路が形成されないので、回路部が生成した出力値は

20

【0038】

図7は、擬似ランダム・クロック信号を生成するのに用いてよい型の線形フィードバック・シフト・レジスタを示す。このようなクロック信号は図5のランダム・クロック日付回路(random clock dating circuit)72に与えられる。異なる回路部には別個の擬似ランダム信号発生器を設けてよい。異なる擬似ランダム発生器に関連する固定クロック周波数を変えて関連する回路部の特性を一致させ、更に必要に応じて隠蔽動作を隠してよい。

【0039】

図8は、回路部の可能信号の制御の概要を示す。ステップ88で、命令復号器68から可能信号enを受けたかどうか判定する。このような可能信号を受けた場合は、処理はステップ90に進む。命令復号器68からの可能信号は、復号された真のプログラム命令に従って、要求された処理演算を行うことが必要であることを示す。したがってステップ90では、関係する回路部への入力と出力とクロック信号とを可能にする。ステップ88で命令復号器から可能信号enを受けない場合は、処理はステップ92に進んで、その回路部のダミー演算が許されるかどうか判定する。ダミー演算が許される場合は、処理はステップ94に進み、回路部への入力とクロックとは可能になるが、回路部からの出力は可能にならない。次に回路部はダミー活動を行う。ステップ92での判定の結果、システム構成パラメータの指示によりダミー演算が許されない場合は、ステップ94をバイパスして処理は終了する。

30

40

【0040】

認識されるように、図8に示すプロセスは順次流れ図の形である。実際には、この制御は異なる順序で行われて、データ処理装置52全体に広がる回路要素を用いてよい。順次に実行されるように示されている動作も実際は並列に実行されてよくまたは制御機能は修正されてよい。全体レベルでは、個別の回路部は、該当するプログラム命令に応じて通常要求される動作を行うことが可能になり、また関連する構成パラメータにより許される場合はダミー活動を行うことが可能になる。

【0041】

図9はレジスタ・バンク96の略図を示す。このレジスタ・バンクは、英国キャンブリッジのARM社が設計したプロセッサに従う、ユーザ・モード動作のARMプロセッサ

50

・プログラマのモデルに基づくものである。実際には、他のプロセッサ・モードについて更にレジスタを用いることがあるが、簡単のために省略した。通常のデータ・レジスタR 0からR 15はデータ値を保持するのに用いる。レジスタR 13, R 14, R 15は、一般に機密保護に関係ないデータ値であるプログラム・カウンタ値、分岐復帰アドレス値、スタック・ポインタを記憶する。したがって、R 13, R 14, R 15についてはデータ書込みの際の移行バランスは必要ない。トラッシュ・レジスタR Tは、その条件コードを失敗した条件付き書込みに関連して用いるためにレジスタ・バンク96内に設けられる。その条件コードを失敗した条件付き書込み命令は、通常は書込みは行わない。しかしこの装置では、このような失敗した条件付き書込み命令は、条件コードを失敗したにもかかわらずやはりトラッシュ・データ・レジスタR Tにデータ値を書き込む。これにより、条件付き書込み動作の条件コード失敗または条件コード合格に付随するはずの電力消費やタイミングの違いを全て隠す。トラッシュ・データ・レジスタR Tは、命令内のレジスタ指定オペランドでアドレス指定できるような方法ではプログラマのモデルに現れない。

10

【0042】

トラッシュ・データ・レジスタR Tだけでなく、高から低へと低から高への移行のバランスをとるために別のレジスタ98, 100も設けられる。専用のダミー・レジスタ98は、トラッシュ・データ・レジスタR Tだけでなくデータ・レジスタR 0からR 12に関して設けられる。共用ダミー・レジスタ100は、移行バランス技術に従ってデータ・レジスタへの書込みのたびに応答して排他的OR値と排他的OR値の逆とを記憶するために設けられる。レジスタ書込み制御回路102は、データ・レジスタへのデータ値の書込みに応じて別のレジスタ98, 100に書き込む該当するデータ値を生成する。この対称的書込み制御は、システム構成コプロセッサ72からの該当するシステム構成制御フラグ信号により選択的に可能または使用禁止になる。

20

【0043】

図10はレジスタ書込み制御回路102の動作の概要を示す流れ図である。ステップ104で、回路はレジスタ書込み動作の命令を待つ。ステップ106で、このレジスタ書込み先が、対称的書込み制御装置が適用されるデータ・レジスタの1つかトラッシュ・データ・レジスタR Tかを判定する。レジスタ書込み先がこれらのレジスタでない場合は処理はステップ108に進み、要求されたデータ値XがレジスタR 13, R 14, R 15の1つに単に書き込まれる。

30

【0044】

書込みが行われるレジスタが対称的レジスタ書込みに従う可能性がある場合は、ステップ110で現在この機能が可能かどうか判定する。現在この機能が可能でない場合は、処理はステップ108に進む。この機能が可能な場合は、処理はステップ112に進む。

【0045】

ステップ112で、レジスタ制御回路はデータ値内のビット位置毎に、その位置に書き込まれた現在のビットとその位置に前に記憶されたビットとの逆排他的ORの値を計算し、次にこれと、そのビット位置に前に記憶されたダミー・レジスタ値との排他的ORをとる(図11を参照)。またレジスタ制御回路102は、この決定の逆と、データ値としてデータ・レジスタに書き込まれたビットの逆も計算する。これらの値を、書き込まれる全てのビットについて計算する(例えば、3ダミー32ビット値)。

40

【0046】

ステップ114で、ステップ108と同様にしてデータ値をデータ・レジスタに書き込む。ステップ116で、関係するレジスタ内のビット位置毎に決定された別の3つの値を別の3レジスタに書き込む。ステップ114と116とは同時に行う。図11に関して説明するように、これにより高から低へと低から高への遷移の数と消費電力のバランスが得られる。

【0047】

図11はデータ書込み動作の前と後の可能なビット値の表を示す。データ値はレジスタR nに書き込まれる。これは対称的書込み動作機能が適用されるレジスタである。時刻t

50

と時刻 $t + 1$ での値が示されている。これらの値の逆は簡単に決定される。この対称的動作に従う各データ・レジスタに対して、現在データ・レジスタ内に保持されているデータ値の逆を記憶する専用のダミーレジスタ 98 が設けられる。

【0048】

共用ダミー・レジスタ 100 は図 11 にはレジスタ R d で示されている。共用ダミー・レジスタ R d 内のビット位置毎に、データ書込みが起こったときにそのビット位置に書き込まれる新しい値が、図 11 の下部に示す関数で決定される。この関数により、データ値とデータ値の逆とに変化が起こらないときは、共用ダミー・レジスタ内の対応するビットとその逆とに、確かに変化が起こる。この表は、データ値が変化しないときに起こる共用ダミー・レジスタ値の変化と、データ値が変化したときに変化しないダミー・レジスタ値 10 内の共用値を示す。このように、書込み毎に保証された固定の遷移数がある、すなわち、高から低へと低から高へのバランスされた等しい遷移数がある。

【0049】

図 13 は、書込み動作がその条件コードを失敗したときに書き込みを行うダミー・データ・レジスタ R D の動作を示す流れ図である。ステップ 118 で、制御論理は命令を受けるのを待つ。この制御論理は命令復号器 68 または他の論理でよい。ステップ 120 で、命令がその条件コードを失敗したかどうか判定する。命令コードがその条件コードを失敗しない場合は、通常はステップ 122 に進んで、その命令内のレジスタ・オペランドが指定するレジスタに書き込みを行う。命令がその条件コードを失敗した場合は処理はステップ 124 に進み、ダミー・データ・レジスタ書込みが可能かどうか判定する。これが可能で 20 ない場合は処理は終了する。ダミー・データ・レジスタ書込みが可能な場合は処理はステップ 126 に進み、条件コードを失敗したにもかかわらず、条件コード失敗命令が計算したデータ値がトラッシュ・データ・レジスタ R T に書き込まれる。これにより、条件コード合格か条件コード失敗かに関係なく、電力消費とタイミングとがバランスする。認識されるように、トラッシュ・データ・レジスタ R T も前に説明した遷移バランシング機構に従う。

【0050】

図 13 は、少なくとも複数の命令について多重命令実行機構を備えるデータ処理装置 128 を示す。データ処理装置 128 は、少なくとも複数のジャバ（登録商標）（Java（登録商標））バイトコード命令の本来の実行（native execution）を 30 支援するものである。この型のデータ処理装置と固有の実行は P C T 特許出願第 W O - A - 0 2 / 2 9 5 5 5 号に述べられている。この出願全体と、本来のハードウェア実行と、特に一層複雑なジャバ・バイトコードの選択的ソフトウェア・エミュレーションに関する開示をここに援用する。

【0051】

ジャバ・バイトコード復号器 130 は入力信号により選択的に可能と使用禁止になってよい。ジャバ・バイトコード復号器 130 が使用禁止の場合は、受けたジャバ・バイトコードは、例外的に固有の A R M サム（Thumb）命令集合を用いてジャバ・バイトコードを処理するためのソフトウェア・エミュレーション・コードの実行を開始する。この支援コードは図に示す領域 132 内のメモリ内に記憶される。ジャバ・バイトコード・プログラム 134 もメモリ内に記憶される。ジャバ・プログラムの実行の性質を隠したい場合は、ジャバ・バイトコード復号器 130 に擬似ランダム信号を与えてこの要素を選択的に可能および使用禁止にして、ジャバ・バイトコードの命令実行機構を、混合ハードウェアおよびエミュレーション機構と純粋エミュレーション機構との間で実質的に切り替えてよい。システム構成レジスタ 136 内の構成制御値はジャバ復号器 130 が存在するかどうか、またこのジャバ復号器 130 をランダムに可能および使用禁止にすることが許されるかどうかを指定する。 40

【0052】

図 14 は、受けたジャバ・バイトコードの処理の概要を示す。ステップ 138 でジャバ・バイトコードを受ける。ステップ 140 で、ジャバ復号器 130 が可能かどうか判定す 50

る。ジャバ復号器 130 を擬似ランダムに可能および使用禁止にすることにより、バイトコードを必ずエミュレートするステップ 142 かまたはハードウェアで命令を実行するステップ 146 に実質的に分岐する。これにより、ジャバ・バイトコード実行に付随する電力シグネチャが隠される／マスクされる。ステップ 146 で、関係する特定のジャバ・バイトコードがジャバ復号器 130 で支援されないと判定されると、ステップ 142 でこのジャバ・バイトコードもソフトウェアでエミュレートされる。しかしジャバ・バイトコードがハードウェアで支援される場合は、ステップ 146 でハードウェアで実行される。

【図面の簡単な説明】

【0053】

本発明の実施の形態について単なる例であるが添付の図面を参照して説明する。

10

【図 1】固定タイミング・モードと可変タイミング・モードとで動作するデータ処理装置の略図を示す。

【図 2】条件付きプログラミング命令の概要を示す。

【図 3】本発明の技術に従って動作する命令復号器が実行する処理動作の一部を示す概略の流れ図である。

【図 4】固定タイミング・モードにおける条件付き分岐命令の実行の概要を示す。

【図 5】選択的に可能になって要求された処理動作またはダミー処理動作を実行する多数の回路部を含むデータ処理装置を示す略図である。

【図 6】要求された可能信号とランダム・ダミー活動可能信号とに依る、回路部とその関連するダミー活動可能回路との概略を示す。

20

【図 7】擬似ランダム信号発生器として用いてよい線形シフト・フィードバック・レジスタを示す略図である。

【図 8】要求された処理活動とダミー処理活動とを実行する回路部の制御の概要を示す流れ図である。

【図 9】条件付き書込み動作がその条件コードを失敗したときにダミー・レジスタ書込みが行われる宛先の多数のデータ処理レジスタと、多数のダミー・レジスタと、多数の共用ダミー・レジスタと、マップされないトラッシュ・レジスタ R T とを含むレジスタ・バンクの一部を示す略図である。

【図 10】レジスタ書込みが生じたときに起こる高から低へと低から高への移行の数をバランスさせようとするレジスタ書込み制御回路の概要を示す流れ図である。

30

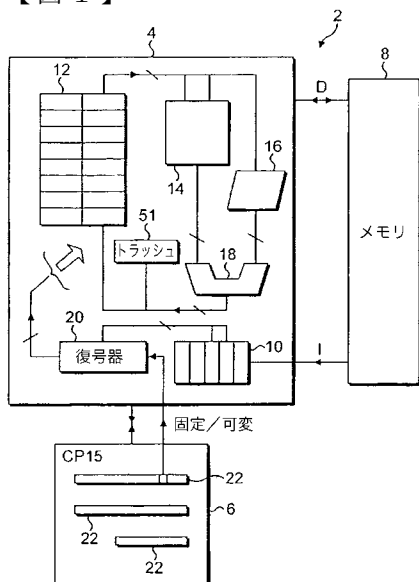
【図 11】レジスタ書込みに関連して起こる高から低へと低から高への移行をバランスさせるよう形成された、データ・レジスタと 3 個の別のレジスタ内の特定のビットのビット移行の関係とを示す表である。

【図 12】書込み動作の条件コード失敗のときのトラッシュ・レジスタへの書込みの制御の概要を示す流れ図である。

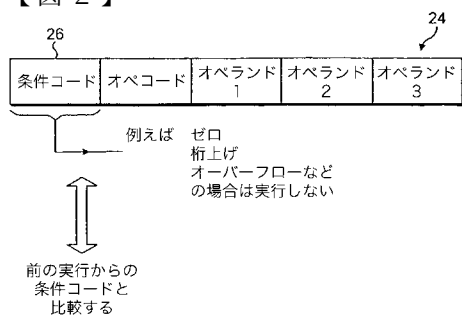
【図 13】命令の多重実行機構と、少なくとも複数の命令に用いられる実行機構の擬似ランダム選択とを有する装置を示す略図である。

【図 14】図 13 の装置の制御の概略を示す流れ図である。

【图 1】

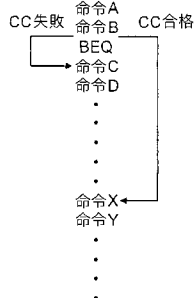


【图 2】

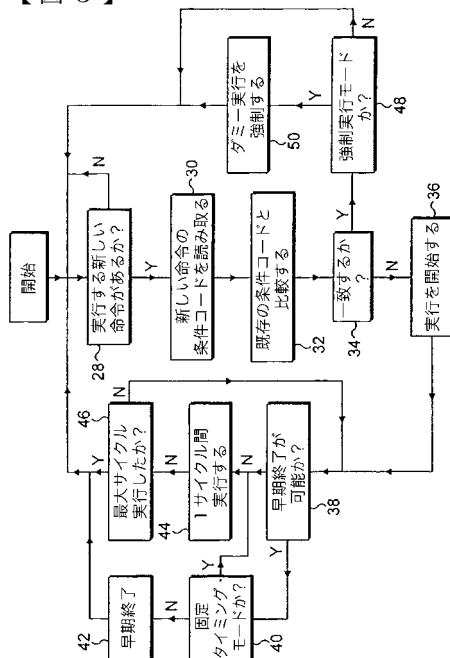


【图 4】

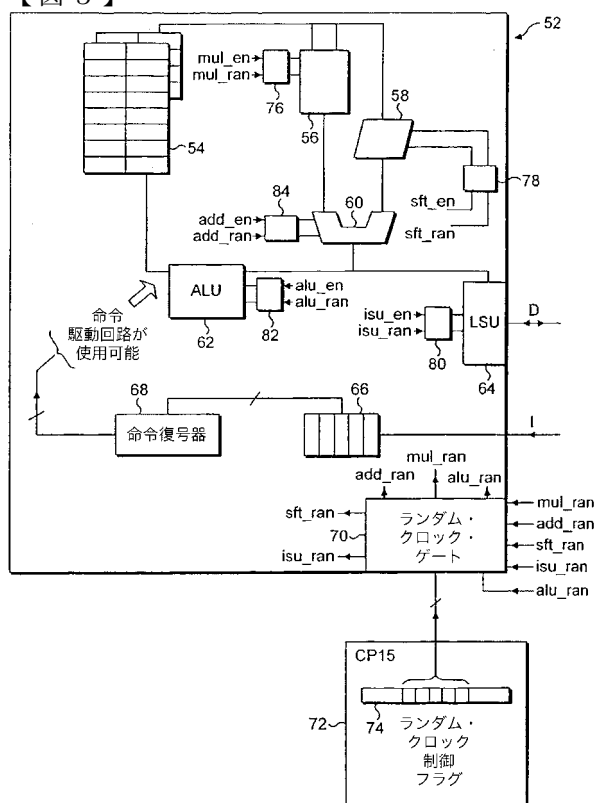
固定タイミング・モード
での条件付き
分岐



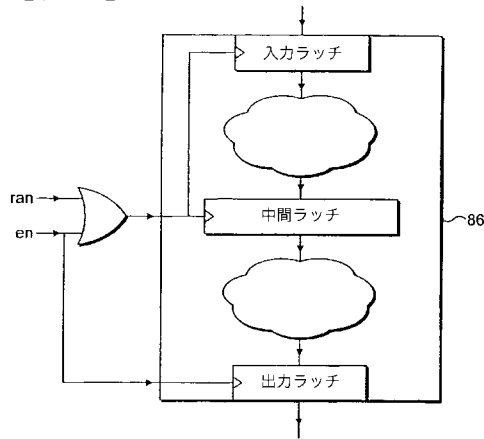
【图 3】



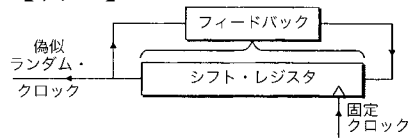
【図 5】



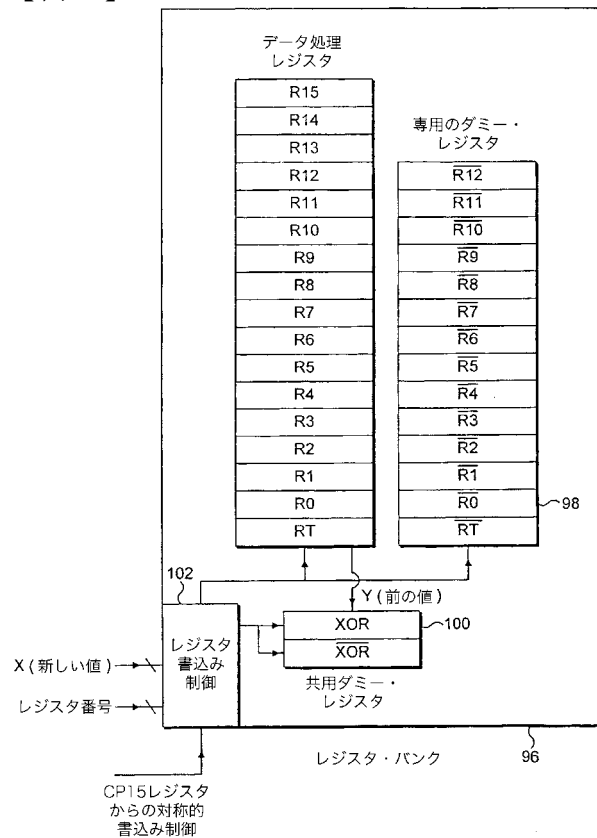
【図 6】



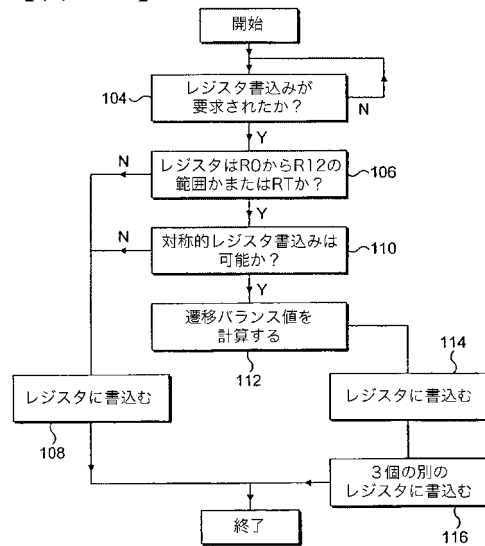
【図 7】



【図 9】



【図 10】

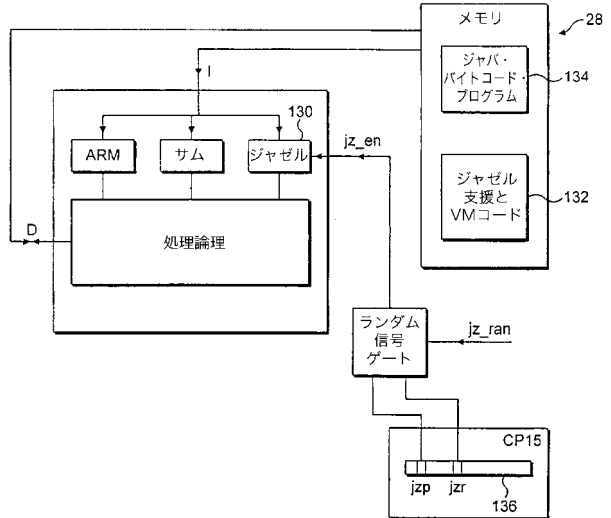


【図 1 1】

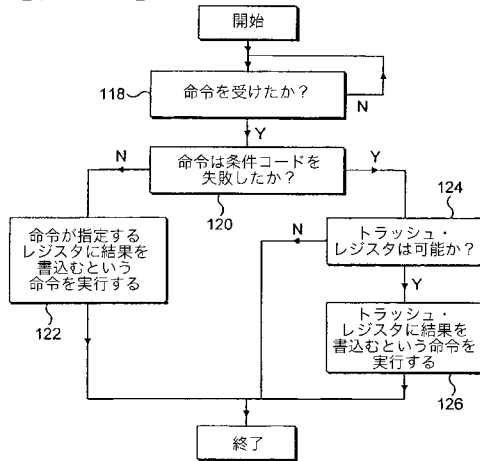
Rn[i]t	Rn[i]t+1	Rn[i]t		Rd[i]t	Rd[i]t+1			遷移			
		Rn[i]t	Rn[i]t+1		Rd[i]t	Rd[i]t+1	Rd[i]t	Rn	Rn	Rd	Rd
0	0	1	1	0	1	1	0	—	—	↑	↓
0	0	1	1	1	0	0	1	—	—	↓	↑
0	1	1	0	0	0	1	1	↑	↓	—	—
0	1	1	0	1	1	0	0	↑	↓	—	—
1	0	0	1	0	0	1	1	↓	↑	—	—
1	0	0	1	1	1	0	0	↓	↑	—	—
1	1	0	0	0	1	1	0	—	—	↑	↓
1	1	0	0	1	0	0	1	—	—	↓	↑

$$Rd[i]t+1 = (Rn[i]t \text{ XOR } Rn[i]t+1) \text{ XOR } Rd[i]t$$

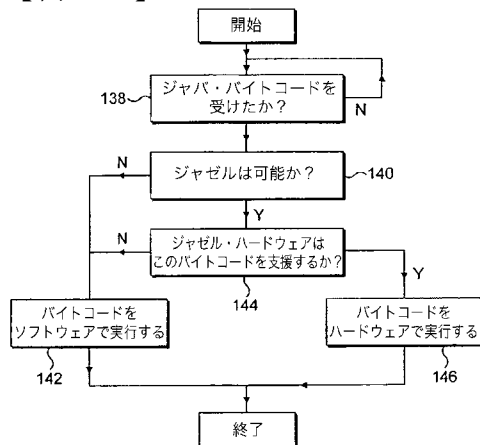
【図 1 3】



【図 1 2】



【図 1 4】



フロントページの続き

(31)優先権主張番号 0302646.5

(32)優先日 平成15年2月5日(2003.2.5)

(33)優先権主張国 英国(GB)

(31)優先権主張番号 0307823.5

(32)優先日 平成15年4月4日(2003.4.4)

(33)優先権主張国 英国(GB)

(72)発明者 ワット、サイモン、チャールズ

イギリス国、ケンブリッジ、バーウエル、 マンデヴィル、ザ タン ハウス

審査官 後藤 彰

(56)参考文献 特表2004-522221 (JP, A)

特開2001-266103 (JP, A)

特開平7-239837 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 9/30 - 9/355