Генератори
на
случайни последователности
в
паралелна изпълнителна среда

Генератори на случайни последователности в паралелна изпълнителна среда

Милен Луканчевски

Русенски университет "Ангел Кънчев"

УДК 004.272 + 004.421.5 + 519.688

Генератори на случайни последователности в паралелна изпълнителна среда

Рецензенти: **проф. д.т.н Райчо Иларионов, ТУ-Габрово**
доц. д-р Лидия Георгиева, РУ "А. Кънчев"

Компютърна обработка: **д-р инж. Милен Луканчевски**

Националност на автора: **българска**
Език на изданието: **български**
Тип (жанр): **научен, монография**
Поредност: **първо**

ISBN 978-619-7071-26-9

Формат 64 x 90/16

Издателски център на Русенския университет "А. Кънчев", 2013.

На лицевата корица: Елементи от екрана на паралелната развойна среда *xTIMEcomposer Studio* на фирмата *XMOS*.

На задната корица: Част от опитната постановка, използвана за изследване и експериментиране с предложените реализации на генератори на случайни последователности.

Изследването и изданието са финансирани от автора и от ръководеното от него научно развойно направление "*Компютърни телекомуникационни системи*".

На мислещите компютърни специалисти,
призвани да преодолеят третата сингулярност

ПРЕДИСЛОВИЕ

Главните направления на развитие на компютърните архитектури на съвременния етап включват постепенен преход от последователния фонноймановъм паралелния изчислителен модел, както и изследването на възможностите за използване принципите на квантовата механика за съхранение, обработка и пренос на информацията.

Предпоставка за работите и при двете направления са физическите ограничения на класическия последователен изчислителен модел. Но докато при първото направление тези ограничения се преодоляват на макониво, то при второто направление стремежът е да се използва скрития на квантово ниво потенциал за паралелна обработка.

От началото на 90-те години в катедра "Компютърни системи и технологии" на Русенския университет "А. Кънчев" се работи в областта на паралелните компютърни системи, което в голяма степен е стимулирано от резултатите в дисертационния труд на автора. Изследванията се основават на паралелния изчислителен модел *CSP* на Чарлз Хоар. Като елементна база са използвани скаларни микропроцесори с общо предназначение.

От 2009 година, както в изследователската, така и в учебната работа, авторът експериментира с новата *SMT/TLP* архитектура *XS1* на фирмата *XMOS*.

Като резултат от осмислянето на получените резултати и на основното противоречие в областта на компютърните архитектури и системи, авторът започва да развива от 2012 година тематика за изследване на квантовите явления чрез моделирането им в паралелна изпълнителна среда.

Възприет за водещ методологичен принцип е съвместното разглеждане на двете главни направления на развитие на компютърните архитектури: на макониво и на квантово ниво. Акцентира се върху изоморфизма на изображението на структурата на изследвания обект или явление в модел с глобален структурен паралелизъм. Оттук произтича и избора на изпълнителната среда с глобален структурен паралелизъм *XCORE/XC*, базирана на *SMT/TLP* архитектура *XS1*.

Като инициатор и ръководител на тези изследвания, авторът

се счита длъжен да представя в монографична форма най-съществените резултати от всеки отделен, логически завършен техен етап.

Предмет на тази монография са основните резултати от първия етап от изследванията, посветен на генераторите на случайни последователности в паралелната изпълнителна среда *XCORE/XC*.

Едновременно излиза от печат и другата монография, в която се обобщават резултатите от втория етап на изследванията - структурното моделиране на ключовите квантови явления поляризация, суперпозиция, квантова телепортация и сплитане [9].

По въпроси, свързани със съдържанието на работата, може да се обръщате на електронната поща mil@ieee.org на автора.

+++

Използвам случая да благодаря на своите студенти, участвали в работите. Най-вече на маг. инж. Бисер Николов за неговия младежки плам и отдаденост на професията.

Възможността за провеждане на изследванията се дължат на подкрепата, която срещам от научно-изследователското направление “Компютърни телекомуникационни системи“ към катедра ”Компютърни системи и технологии” на Русенския университет “А. Кънчев“.

Рецензентите на представената работа - проф. д.т.н. Райчо Иларионов и доц. д-р Лидия Георгиева поеха с желание отговорността да помогнат за повишаване на нейното ниво чрез своите бележки, коментари и препоръки.

Благодаря на майка си - моят най-верен приятел, вдъхновител и ориентир!

Милен Луканчевски,
IEEE Computer Society,
IEEE Communications Society & ACM Member

Русе, октомври 2013 г.

СЪДЪРЖАНИЕ

СПИСЪК НА ФИГУРИТЕ И ТАБЛИЦИТЕ

СПИСЪК НА СЪКРАЩЕНИЯТА

CSP - Communicating Sequential Processes (Взаимодействащи последователни процеси)

CRC – Cyclic Redundancy Check (Цикличен контролен код, Полиномиален контролен код)

DLP – Data Level Parallelism (Паралелизъм на ниво данни)

DSP – Digital Signal Processor/Digital Signal Processing (Процесор за цифрова обработка на сигналите/Цифрова обработка на сигналите, ЦОС)

ILP - Instruction Level Parallelism (Паралелизъм на ниво инструкции, локален паралелизъм, базиран на конвейеризацията на инструкциите)

JTAG – Joint Test Action Group (Стандартен интерфейс за връзка между инструменталната и целевата машина)

LCG – Linear Congruental Generator (Линеен конгруентен генератор)

LFSR – Linear Feedback Shift Register (Изместващ регистър с линейна обратна връзка)

MAC – Multiply And Accumulate (сложен оператор от вида „Умножи и натрупай", популярен при DSP)

MLCG – Multiplicative Linear Congruental Generator (Мултипликативен линеен конгруентен генератор)

MPP – Massively-Parallel Processor (Масово-паралелен процесор)

MTP - Multithreading Parallelism (многонишков паралелизъм, паралелизъм на ниво нишки)

OCCAM – ОККАМ (Език за паралелно програмиране, базиран на CSP)

OSI – Open Systems Interconnection (Теоретичен модел, описващ принципния начин на комуникация и строежа на компютърните мрежи)

OTP – Once-Time Programmable Memory (Постоянна памет, ROM)

PHY - Physical Layer (Физическото ниво от OSI модела)

PRNG – Pseudo-Random Number Generator (Генератор на псевдослучайни числа)

RISC – Reduced Instruction Set Computer (Компютър с опростена система инструкции)

RNG – Random Number Generator (Генератор на случайни числа)

RRNG – Real Random Number Generator (Генератор на действително-случайни последователности)

SMT - Simultaneous Multithreading (Едновременно многонишково изпълнение; общоприето название на апаратната технология, позволяваща едновременното изпълнение на няколко нишки; фирмата Intel използва обозначението Hyperthreading)

SPI – Serial Peripheral Interface Bus (Сериен периферен инртерфейс)

SRAM – Static Random-Access Memory (Статична памет с произволен достъп)

STL - Standard Template Library (Стандартна библиотека от шаблони на C++)

TLP – Task Level Parallelism (Паралелизъм на ниво задачи)

TRNG – True Random Number Generator (Генератор на действително-случайни последователности)

UVLSI – Ultra Very Large Scale Integration (СГИС, Свръхголеми интегрални схеми)

USB – Universal Serial Bus (Универсална серийна шина)

VLIW – Very Large Instruction Word (RISC архитектура с много голяма дължина на инструкцията; един от методите за явен ILP)

VLSI – Very Large Scale Integration (ГИС, Големи интегрални схеми)

XC – XMOS C (паралелна версия на езика C за архитектурата XS1 на фирмата XMOS, разширение на езика C с паралелни конструкции, повечето от които се поддържат директно на апаратно ниво)

XCORE - паралелно ядро от фамилията *XS1* на фирмата XMOS с глобален структурен паралелизъм; физическа реализация на CSP-машина с апаратна поддръжка на паралелизма

XCORE/XC - паралелна платформа на фирмата XMOS, базирана на паралелната архитектура XCORE и на езика за паралелно програмиране XC

XDE – XMOS Development Environment (Название на развойната среда на фирмата XMOS до версия 11; от версия 12 е част от окрупнената развойна среда *xTIMEcomposer Studio* на фирмата XMOS)

XOR – Exclusive Or (Изключващо ИЛИ)

XS1 - Фамилия паралелна архитектура от типа XCORE на фирмата XMOS