вирусов / Защита информации Сб. н. т. НАУ - 2004 Выпуск 11, с. 87 – 96. ***7.*** *Круглов В. В., Борисов В. В. Искусственные нейронные сети. / М.: Горячая линия-Телеком, 2002. – 382 с.* ***8.*** *Каллан Р. Основные концепции нейронных сетей. // М.: Вильямс, 2003. – 288 с.*

УДК 621.391

ОЦЕНКА СЛОЖНОСТИ РЕАЛИЗАЦИИ АЛГОРИТМОВ ДЕКОДИРОВАНИЯ ТУРБОКОДОВ ПРИ ДЕКОДИРОВАНИИ БИТА ИНФОРМАЦИИ НА ЦИФРОВЫХ СИГНАЛЬНЫХ ПРОЦЕССОРАХ

Сергей Зайцев, Сергей Ливенцев, Борис Горлинский
Специальный факультет СБ Украины ВИТИ НТУУ "КПИ"

Анотація: **Проведено оцінку складності декодування біта інформації при апаратно-програмній реалізації турбокодів на цифрових сигнальних процесорах. Розглянуто Map, Max Log Map та Log Map алгоритми декодування турбоходів.**
Summary: **In the article the analysis of complexity of decoding the information bit is made at hardware-software realization turbocodes on digital signal processors. Are considered Map, Max Log Map and Log Map algorithms of decoding turbocodes.**
Ключові слова: **Турбокоди, цифрові сигнальні процесори, алгоритми декодування.**

I Введение

Турбокоды (ТК) обладают высокими корректирующими свойствами при низких отношениях сигнал-шум в канале связи, могут быть реализованы программным, аппаратным или программно-аппаратным способом. Как правило, практически ТК реализуются программно-аппаратным способом на цифровых сигнальных процессорах (ЦСП) [1, 2]. В качестве ЦСП широко используется высокопроизводительный 32-разрядный процессор ADSP-2106x семейства ADSP-21000 с плавающей точкой, который используется для обработки речи, графики, звука и др. Процессоры семейства ADSP-21000 выполняют все команды за один цикл. Они поддерживают высокую тактовую частоту, а также полный набор арифметических операций, включающий помимо традиционных умножения, сложения, вычитания и комбинированного умножения/сложения, примитивы деления ($1/x$ и $\sqrt{10}$), сравнения, определения абсолютного значения, операции min, max, Shift (арифметический сдвиг), Rotate (циклический сдвиг) и др. [3, 4]. Практически все они являются общими и для других семейств высокопроизводительных процессоров. Все вычислительные операции выполняются в арифметико-логическом устройстве, умножителе и устройстве сдвига вычислительного устройства ЦСП.

Наиболее сложным элементом в структуре ТК является декодер, который использует для декодирования специальные алгоритмы. За оценку сложности алгоритмов декодирования ТК в работе принято количество элементарных операций, необходимых для декодирования одного бита информации ЦСП.

II Постановка задачи

Анализ работ [5 – 8] показывает, что при оценке сложности декодирования одного бита информации не полностью учитывалось количество проверочных символов с выхода рекурсивного систематического сверточного кодера (РССК), обязательное использование нормализации, а основные алгебраические операции не были полностью представлены как элементарные. В связи с этим возникает задача анализа сложности алгоритмов декодирования ТК с учетом данных особенностей.

Таким образом, **целью работы** является аналитическое описание и сравнительный анализ сложности реализации декодирования бита информации при использовании *Map, Max Log Map* и *Log Map* алгоритмов декодирования ТК по показателю количества элементарных операций.

Данная статья является продолжением работы [8], в которой получена оценка количества

алгебраических операций, которые необходимо выполнить для декодирования бита информации. При этом основными операциями являются: операции сложения (ADD), умножения (MULT), деления (DIV), вычитания (SUB), определение максимального значения (MAX), сравнения (COMP) и определения абсолютного значения (ABS) двух чисел, а также логарифмирование (LOG) и экспоненцирование (EXP).

III Количество алгебраических операций для декодирования бита информации по алгоритмам *Map, Max Log Map* и *Log Map*

В табл. 1 – 3 показаны сводные данные, полученные в [8] (для *Map, Max Log Map* и *Log Map* алгоритмов декодирования), где m – количество ячеек памяти, а q – общее количество символов с выхода РССК.

Таблица 1 – Количество алгебраических операций для декодирования бита информации по алгоритму *Map*

Операции	**Параметры алгоритма декодирования *Map***							
	γ	α	β	$\tilde{\alpha}$	$\tilde{\beta}$	σ	L	L_e
ADD	$2 \times 2^m \times q$	2^m	2^m	2^m - 1			2×2^m - 2	
MULT	$2 \times 2^m \times (q + 3)$	2×2^m	2×2^m			4×2^m		
DIV				2^m	2^m		1	
SUB								2
LOG							1	
EXP	2×2^m							

Таблица 2 – Количество алгебраических операций для декодирования бита информации по алгоритму *Max Log Map*

Операции	**Параметры алгоритма декодирования *Max Log Map***							
	Γ	A	B	$\tilde{\text{A}}$	$\tilde{\text{B}}$	σ	L	L_e
ADD	$2 \times 2^m \times q$	2×2^m	2×2^m			4×2^m		
MULT	$2 \times 2^m \times (q + 3)$							
SUB				2^m	2^m		1	2
MAX		2^m	2^m	2^m - 1			2×2^m - 2	

Таблица 3 – Количество алгебраических операций для декодирования бита информации по алгоритму *Log Map*

Операции	**Параметры алгоритма декодирования *Log Map***							
	Γ	A	B	$\tilde{\text{A}}$	$\tilde{\text{B}}$	σ	L	L_e
ADD	$2 \times 2^m \times q$	3×2^m	3×2^m			4×2^m	2×2^m - 2	
MULT	$2 \times 2^m \times (q + 3)$							
SUB				2^m	2^m		1	2
MAX		2^m	2^m	2^m - 1			2×2^m - 2	
COMP		5×2^m	5×2^m				10×2^m - 10	
ABS		2^m	2^m				2×2^m-2	

Полученные алгебраические операции соответствуют выполняемым за цикл работы ЦСП, кроме деления, логарифмирования и экспоненцирования. Поэтому для анализа экспоненты и логарифма воспользуемся разложением функций $e^x, x \in (-\infty;\infty)$ и $\ln\frac{1+x}{1-x}, x \in (-1;1]$ в степенной ряд [10], а деление $\frac{a}{b}$ представим как $a \cdot \frac{1}{b}$ (операция $\frac{1}{b}$ (RECIPS) соответствует элементарной для ЦСП [3]).

С учетом данных преобразований алгебраические операции табл. 1, как выполнимые за один такт работы сигнальным процессором, представлены в табл. 4. Операции табл. 2, 3 остаются без преобразований, т. к. они соответствуют элементарным.

Таблица 4 – Количество элементарных операций для декодирования бита информации по алгоритму *Map*

Операции	Параметры алгоритма декодирования *Map*							
	γ	α	β	$\tilde{\alpha}$	$\tilde{\beta}$	σ	L	L_e
ADD	$2 \times 2^m \times q + 22 \times 2^m + 8$	2^m	2^m	$2^m - 1$			$2 \times 2^m - 2$	
MULT	$2 \times 2^m \times q + 246 \times 2^m + 66$	2×2^m	2×2^m	2^m	2^m	4×2^m	1	
RECIPS	$20 \times 2^m + 8$			2^m	2^m		1	
SUB	1							2

IV Оценка сложности реализации алгоритмов декодирования *Map, Max Log Map* и *Log Map* на цифровых сигнальных процессорах

Суммированием получим общее количество элементарных операций для рассмотренных алгоритмов декодирования, необходимых для декодирования одного бита информации.

В результате, сложность декодирования бита информации по показателю элементарных операций для соответствующих алгоритмов декодирования определяется следующими формулами:

$$\phi_{Map} = 4 \times 2^m \times q + 305 \times 2^m + 84 \quad (1)$$

$$\phi_{Max\ Log\ Map} = 4 \times 2^m \times q + 21 \times 2^m \quad (2)$$

$$\phi_{Log\ Map} = 4 \times 2^m \times q + 49 \times 2^m - 14. \quad (3)$$

Следовательно, сложность алгоритмов декодирования ТК (ϕ) является функцией от количества ячеек памяти РССК и количества символов на выходе РССК: $\phi_{Map} = f(m, q)$, $\phi_{Max\ Log\ Map} = \xi(m, q)$, $\phi_{Log\ Map} = \zeta(m, q)$.

Используя (1), (2), (3), получим оценку количества элементарных операций, которые необходимо выполнить сигнальному процессору для декодирования бита информации при использовании РССК различного вида в составе кодера турбокода, соответственно для *Map, Max Log Map* и *Log Map* алгоритмов декодирования. Данные значения представлены в табл. 5 – 7, для различного количества m и q.

Таблица 5 – Количество элементарных операций при декодирования бита информации для *Map* алгоритма

	q			
m	2	3	4	5
2	1336	1352	1368	1384
3	2588	2620	2652	2684
4	5092	5156	5220	5284
5	10100	10228	10356	10484
6	20116	20372	20628	20884
7	40148	40660	41172	41684
8	80212	81236	82260	83284
9	160340	162388	164436	166484

Таблица 6 – Количество элементарных операций при декодирования бита информации для *Max Log Map* алгоритма

	q			
m	2	3	4	5
2	116	132	148	164
3	232	264	296	328
4	464	528	592	656
5	928	1056	1184	1312
6	1856	2112	2368	2624
7	3712	4224	4736	5248
8	7424	8448	9472	10496

9	14848	16896	18944	20992

Таблица 7 – Количество элементарных операций при декодировании бита информации для *Log Map* алгоритма

	q			
m	2	3	4	5
2	214	230	246	262
3	442	474	506	538
4	898	962	1026	1090
5	1810	1938	2064	2194
6	3634	3890	4146	4402
7	7282	7794	8306	8818
8	14578	15602	16626	17650
9	29170	31218	33266	35514

Зависимость сложности *Map, Max Log Map* и *Log Map* алгоритмов декодирования от количества ячеек памяти РССК для различных *q* представлена соответственно на рис. 1 – 3.

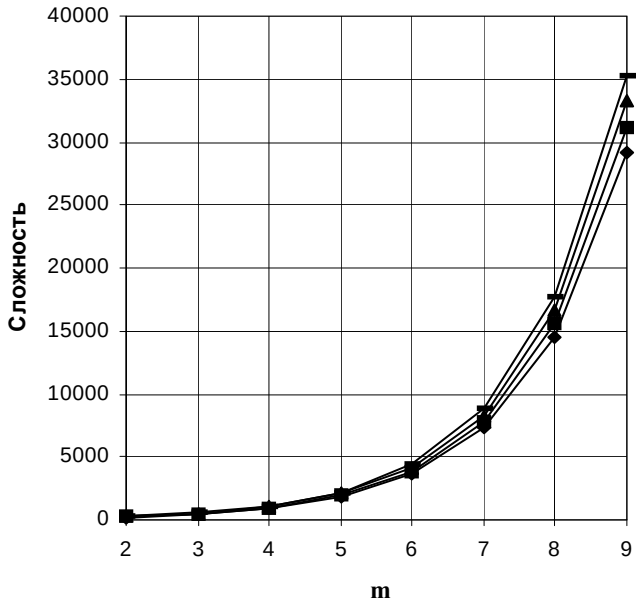

Рисунок 3

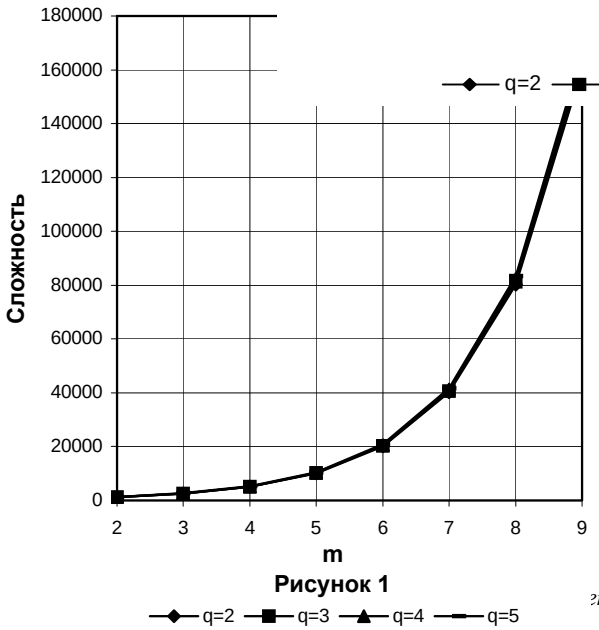

Рисунок 1

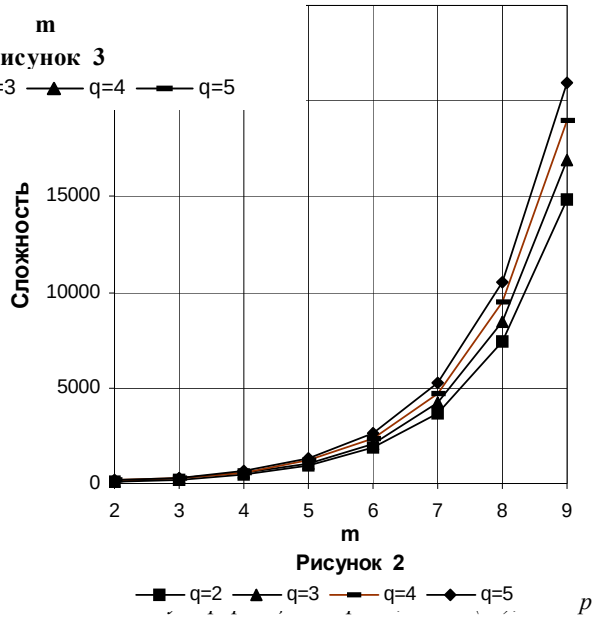

Рисунок 2

Анализ рисунков свидетельствует о том ,что сложность реализации алгоритмов декодирования ТК возрастает єкспоненніально с увеличением m РССК, а с возрастантем q – незначительно, кроме того, видно, что при одинаковых исходных данных более сложным является Map алгоритм, а менее сложным – Max Log Map.

Для сравнения алгоритмов воспользуемся параметрами относительной сложности n, n_1 и n_2. Параметр n показывает, во сколько раз алгоритм *Map* сложнее *Max Log Map*, а n_1 – соответсвенно *Log Map*. Параметр n_2 определяет, во сколько раз *Log Map* сложнее *Max Log Map* алгоритма.

$$n\cdot(4\times 2^m\times q+21\times 2^m)=4\times 2^m\times q+305\times 2^m+84 \Rightarrow$$

$$n=\frac{4\times 2^m\times q+305\times 2^m+84}{4\times 2^m\times q+21\times 2^m}, \quad (4)$$

$$n_1\cdot(4\times 2^m\times q+49\times 2^m-14)=4\times 2^m\times q+305\times 2^m+84 \Rightarrow$$

$$n_1=\frac{4\times 2^m\times q+305\times 2^m+84}{4\times 2^m\times q+49\times 2^m-14}, \quad (5)$$

$$n_2\cdot(4\times 2^m\times q+21\times 2^m)=4\times 2^m\times q+49\times 2^m-14 \Rightarrow$$

$$n_2=\frac{4\times 2^m\times q+49\times 2^m-14}{4\times 2^m\times q+21\times 2^m}. \quad (6)$$

В табл. 8 – 10 представлены значения n, n_1 и n_2.

Таблица 8 – Относительная сложность алгоритма *Map* по сравнению с *Max Log Map*

	q			
m	2	3	4	5
2	11,5	10,2	9,2	8,4
3	11,2	9,9	9,0	8,2
4	11,0	9,8	8,8	8,1
5	10,9	9,7	8,7	8,0
6	10,8	9,6	8,7	8,0
7	10,8	9,6	8,7	7,9
8	10,8	9,6	8,7	7,9
9	10,8	9,6	8,7	7,9

Таблица 9 – Относительная сложность алгоритма *Map* по сравнению с *Log Map*

	q			
m	2	3	4	5
2	6,2	5,9	5,6	5,3
3	5,9	5,5	5,2	5,0
4	5,7	5,4	5.1	4,8
5	5,6	5,3	5,0	4,8
6	5,5	5,2	5,0	4,7
7	5,5	5,2	5,0	4,7
8	5,5	5,2	5,0	4,7
9	5,5	5,2	5,0	4,7

Таблица 10 – Относительная сложность алгоритма *Log Map* по сравнению с *Max Log Map*

	q			
m	2	3	4	5
2	1,8	1,7	1,7	1,6
3	1,9	1,8	1,7	1,6
4	1,9	1,8	1,7	1,7
5	1,9	1,8	1,7	1,7
6	1,9	1,8	1,7	1,7
7	1,9	1,8	1,8	1,7
8	1,9	1,8	1,8	1,7
9	1,9	1,8	1,8	1,7

V Выводы

- Для адекватного сравнения сложности реализации различных алгоритмов декодирования ТК алгебраические операции, необходимые для декодирования бита информации, должны быть представлены как элементарные для ЦСП.
- Сравнительный анализ алгоритмов декодирования показал, что самым сложным является *MAP* алгоритм, т. к., например, при $m = 3$ и $q = 3$ сложность этого алгоритма равна $\phi = 2620$ элементарных операций, и, как показал дальнейший анализ, он в 9,9 раза сложнее *Max Log Map* алгоритма и в 5,5 раза *Log Map* алгоритма.
- Полученные выражения целесообразно использовать для анализа сложности реализации кодера и декодера ТК на типовых ЦСП с целью выбора элементной базы для реализации ТК.

Литература: ***1.*** *Gracie K., Crozier S., Hunt A. Performance of a Low-Complexity Turbo Decoder with a Simple Early Stopping Criterion Implemented on a SHARC Processor // Communications Research Centre (*http://www.crc.ca/fec*).* ***2.*** *Gracie K., Crozier S., Hunt A. Performance of a Low-Complexity Turbo Decoder and its Implementation on a Low-Cost, 16-Bit Fixed-Point DSP // Communications Research Centre (http://www.crc.ca/fec).* ***3.*** *Руководство пользователя по сигнальным процессорам семейства SHARC ADSP-2106 x // Пер. с англ. Бархатов А. В., Коновалов А. А., Петров М. Н. ООО ЭЛТЕХ г. Санкт-Петербург. – 2002. С. 493 – 539.* ***4.*** *Srinivas K. Low-Cost Simd SHARC // Analog Devices, 2001. – P. 24 – 25 (http://www.analog.com/processors).* ***5.*** *Robertson P., Villebrun E., Hoeher P. Optimal and sub-optimal maximum a posteriori algorithms suitable for turbo decoding // Institute of communications technology. – Oberpfaffenhofen, Germany. – P. 4 – 9, 14.* ***6.*** *Malardel F. Simulation and Optimisations of the Turbo Decoding Algorithm // Signal Processing Research Institute – University of South Australia, 1996. – July-November. – P. 23 – 26.* ***7.*** *Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник // Москва: Горячая линия – Телеком. – 2001. С. 104.* ***8.*** *Ливенцев С. П., Зайцев С. В., Горлинский Б. В. Анализ сложности Map, Max Log Map, Log Map алгоритмов декодирования турбокодов при декодировании бита информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 1 (12). – С. 119 – 129.* ***9.*** *Ливенцев С. П., Алексеев Д. А., Зайцев С. В. Анализ характеристик перемежителей, используемых в турбокодах // Зв'язок. – 2005. – № 3. – С. 57 – 61.* ***10.*** *Фильчаков П. Ф. Справочник по высшей математике // "Наукова думка", Киев. – 1972. – 456 с.*

УДК 004.31, 004.056.55, 003.26

СТАТИСТИЧНІ МОДЕЛІ ДВОМІСНИХ ЛОГІЧНИХ ОПЕРАЦІЙ ДЛЯ ПРОВЕДЕННЯ ІНЖЕНЕРНО-КРИПТОГРАФІЧНИХ АТАК ЗА ПОБІЧНИМИ КАНАЛАМИ ВИТОКУ ІНФОРМАЦІЇ

Микола Карпінський*, Леся Коркішко

**Університет в Бєльську-Бяла, Польща, Тернопільський державний економічний університет*

Анотація: **Запропоновано статистичні моделі, досліджено їх властивості та запропоновано методику**