ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿՐԹՈՒԹՅԱՆ ԳԻՏՈՒԹՅԱՆ
ՄՇԱԿՈՒՅԹԻ ԵՎ ՍՊՈՐՏԻ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

ՀԱՅԱՍՏԱՆԻ ԱԶԳԱՅԻՆ ՊՈԼԻՏԵԽՆԻԿԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Ապիկյան Ռոբերտ Կարենի

GPS ՀԱՄԱԿԱՐԳԻ ԿՈԴԱՎՈՐՄԱՆ ԱՐԴՅՈՒՆԱՎԵՏ ԱԼԳՈՐԻԹՄՆԵՐԻ ՄՇԱԿՈՒՄԸ և ՀԵՏԱԶՈՏՈՒՄԸ

Ե. 12.03 – «Հեռահաղորդակցական ցանցեր, սարքավորումներ և համակարգեր» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ, КУЛЬТУРЫ И СПОРТА
РЕСПУБЛИКИ АРМЕНИЯ
НАЦИОНАЛЬНЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ АРМЕНИИ

Апикян Роберт Каренович

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ОПТИМАЛЬНЫХ АЛГОРИТМОВ КОДИРОВАНИЯ СИСТЕМЫ GPS

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук по специальности 05.12.03 – «Телекоммуникационные сети, устройства и системы»

Ереван 2020

Ատենախոսության թեման հաստատվել է Հայաստանի Ազգային պոլիտեխնիկական համալսարանում

Գիտական ղեկավար՝ տ.գ.դ. Հ.Ա. Գոմցյան

Պաշտոնական ընդդիմախոսներ՝ տ.գ.դ. Վ. Հ. Ավետիսյան
տ.գ.թ. Դ.Գ. Զարգարյան

Առաջատար կազմակերպություն՝ Կապի միջոցների ԳՀԻ, ք. Երևան, ՀՀ

Ատենախոսության պաշտպանությունը տեղի կունենա 2020թ. հուլիսի 6-ին, ժամը 14:00-ին, ՀԱՊՀ-ում գործող «Ռադիոտեխնիկայի և էլեկտրոնիկայի» 046 մասնագիտական խորհրդի նիստում (հասցե՝ 0009, Երևան, Տերյան փ., 105, 17 մասնաշենք):

Ատանախոսությանը կարելի է ծանոթանալ ՀԱՊՀ-ի գրադարանում:
Սեղմագիրը առաքված է 2020 թ. մայիսի 26-ին:

046 մասնագիտական խորհրդի
Գիտական քարտուղար՝ տ.գ.թ. Մ.Յ. Այվազյան

Тема диссертации утверждена в Национальном политехническом университете Армении

Научный руководитель: д.т.н. О.А. Гомцян

Официальные оппоненты: д.т.н. В.Г. Аветисян
к.т.н. Д.Г. Заргарян

Ведущая организация: НИИ средств связи, г. Ереван, РА

Защита диссертации состоится 6-ого июля 2020 в 14:00 ч. на заседании специализированного совета 046 – “Радиотехника и электроника”, действующего при Национальном политехническом университете Армении (НУПА), по адресу: 0009, г. Ереван, ул. Теряна 105, корпус 17.

С диссертацией можно ознакомиться в библиотеке НПУА.
Автореферат разослан 26-го мая 2020 г.

Ученый секретарь
Специализированного совета 046. к.т.н. М.Ц. Айвазян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В радионавигационной системе GPS генераторы С/А кодов относятся к семейству генераторов псевдослучайных последовательностей, получивших широкое применение в криптографии, для кодировки сигналов и т.д. Использование псевдослучайных последовательностей в радионавигационной системе прежде всего связано с тем, что они обладают высокими корреляционными и автокорреляционными свойствами. Обычно псевдослучайные последовательности имеют более высокую частоту, чем сам информационный сигнал. Радиосигналы GPS передаются на частотах диапазона L (1…2 ГГц) и содержат две составляющие: дальномерные коды на основе псевдослучайных последовательностей и навигационные данные. В системе GPS скорость передачи навигационных данных составляет 50 бит/с, а скорость псевдослучайных последовательностей С/А кодов – 1023 Мбит/с. С/А коды являются уникальными для каждого спутника. Между высокочастотным информационным сигналом и носителем, с частотой 1575,42 МГц, выполняется BPSK модуляция, после чего полученный сигнал передается на антенну спутника. В результате у антенны GPS приемника формируется суммарное поле, которое состоит из сигналов доступных спутников. С целью выявления навигационных данных из суммарного поля, приемник локально генерирует псевдослучайные последовательности С/А кодов для каждого спутника, после чего выполняет корреляцию между генерированными последовательностями и суммарным сигналом. При обнаружении корреляционного пика приемник начинает декодирование навигационных данных.

В работе рассматриваются методы параллельной генерации псевдослучайных последовательностей и способы повышения их корреляционных свойств с помощью генетических алгоритмов. При этом имеется возможность более быстрого обнаружения навигационных сигналов. Исходя из вышеизложенного, тема диссертационной работы является актуальной.

Цель работы. Целью диссертационной работы является исследование типов и методов генерации псевдослучайных последовательностей в радионавигационной системе GPS, а также способов повышения их скорости генерации и корреляционных свойств.

Методы исследования. В диссертационной работе для достижения поставленных целей были применены генетические алгоритмы и программный подход для разработанных алгоритмов.

Научная новизна. В процессе исследования получены следующие научные результаты:

1. Основываясь на генетических алгоритмах, разработана программа, генерирующая последовательности, обладающие высокими автокорреляционными свойствами, с помощью которых были исследованы корреляционные характеристики C/A кодов.
2. В результате исследования работы генератора C/A кодов получены уравнения для параллельной генерации выходных данных линейных регистров сдвига с обратной связью (ЛРСОС) и разработан алгоритм для параллельной генерации выходных последовательностей C/A кодов.
3. Вычислена связь между параметрами ЛРСОС и количеством необходимых регистров для параллельной генерации выходных последовательностей.
4. Выведено уравнение, описывающее связь между параметрами регистра и соотношением времен при параллельной и последовательной генерации выходных последовательностей.
5. Основываясь на исследованиях корреляции сигналов и разработанных алгоритмах параллельной генерации псевдослучайных последовательностей, разработан метод для генерации прерывающихся псевдослучайных последовательностей.
6. Разработаны программные пакеты, которые предоставляют возможность для генерации псевдослучайных последовательностей, работы с ЛРСОС, генерации последовательностей на основе генетических алгоритмов, поочередной и параллельной генерации псевдослучайных последовательностей и корреляции сигналов.

Практическая ценность работы. Разработанные алгоритмы и программы могут быть использованы при проектировании приемников GPS системы с целью быстрого позиционирования и во многих других сферах, где в аппаратных схемах используются генераторы псевдослучайных чисел, такие как BLE (Bluetooth Low Energy), USB 3.0, CDMA и др.

Достоверность научных положений подтверждается получением повышенного быстродействия во время генерации C/A псевдослучайных последовательностей в программной среде, а также соответствием аналитических выводов с результатами работы.

Внедрение. Результаты диссертации внедрены в ЗАО “Рединет”, г.Ереван для моделирования GNSS системы и реализации технологии CDMA.

Основные положения, выносимые на защиту.

1. Программный генератор случайных последовательностей на основе работы генетических алгоритмов, а так же исследование

корреляционных свойств последовательностей с параметрами C/A кодов, сгенерированных с помощью той же программы и их сравнение с корреляционными свойствами псевдослучайных последовательностей C/A кодов.

2. Представленная методика для параллелизации процесса генерации, разработанная в результате исследования ЛРСОС, составляющего основу генератора C/A кода и ее реализация в программной среде.

3. Генерация с прерываниями C/A кодов и выходных последовательностей ЛРСОС и результаты исследования их корреляционных свойств.

4. Разработанные программные приложения, с помощью которых можно проверить и исследовать работу представленных алгоритмических решений.

Публикации. По теме диссертации были опубликованы семь научных работ в армянских, российских и международных журналах IEEE.

Структура и объем работы. Диссертация состоит из введения, четырех глав, основных выводов, списка литературы, включающего 78 наименований. Основной объем работы составляет 125 страницы, включая 75 рисунков и 5 таблиц. Диссертация написана на армянском языке.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы работы, сформулированы цель и основные задачи исследования, представлены научная новизна, практическое значение работы и основные научные положения, выносимые на защиту.

В первой главе осуществлен обзор сигналов старого и нового поколений системы GPS. Приведены описание и характеристики основных видов кодирования сигналов.

1. В настоящее время в навигационной системе GPS передаются 4 типа сигналов для гражданского пользования: L1C/A, L2C, L5IQ, L1C, а также 4 типа сигналов для военного целей: L1P(Y), L2P(Y), L1M, L2M, где первые два символа имени сигнала указывают на номер носителя (L1=1575,42 МГц, L2=1227,60 МГц, L5=1176,45 МГц), а остальная часть - на метод кодировки навигационных данных. Перечисленные типы сигналов можно разделить на два поколения.

В первое поколение входят сигналы, которые присутствовали в системе со дня его старта и в настоящее время поддерживаются и новыми, и старыми

спутниками. Из выше вышеперечисленных сигналов к этому поколению относятся сигналы L1C/A, L1P(Y), L2P(Y).

Генератор C/A кода основан на двух регистрах псевдослучайных последовательностей Фибоначчи. Специальная конфигурация второго регистра дает возможность сгенерировать уникальные последовательности для каждого спутника. Навигационные данные складываются с последовательностями C/A кодов по модулю два, что придает сигналу высокую помехоустойчивость. Скорость генерации последовательностей C/A кодов составляет 1,023 Мбит/с, что намного выше, чем скорость навигационных данных, которая составляет 50 бит/с.

P(Y) код, в отличие от C/A кодов, предназначен для военных приемников. Скорость генерации P(Y) кода составляет 10,23Мбит/с, что в десять раз выше, чем скорость C/A кода. P(Y) код является суммарным кодом и получается в результате складывания P и W кодов. Генерация P кода основана на работе линейного регистра сдвига с обратной связью. Генерация W кода является секретом.

Сигналами нового поколения GPS являются L2C, L5, L1C, L1M и L2M, которые транслируются только новыми спутниками системы. Первые три сигнала L2C, L5, L1C предназначены для гражданского пользования, а сигналы L1M и L2M- для военных целей. Сигнал L2C содержит две последовательности: CM (*civil-moderated*) и CL (*civil-long*). Скорость генерации последовательностей CM составляет 511,500 бит/с, а длина - 10230 бит. Он используется для кодировки навигационной информации. Скорость генерации CL кодов тоже составляет 511,500 бит/с, а длина - 767250 бит. Генерация CM и CL кодов основана на ЛРСОС.

Следующим сигналом для гражданского пользования является L5, который предназначен для применения в авиационной локации. Он состоит из двух псевдослучайных последовательностей: I5 и Q5, где I5 код содержит навигационную информацию, а Q5 код является пилотным и используется приемником только для быстрого обнаружения сигнала спутника. Генераторы обоих компонентов I5 и Q5 тоже основаны на ЛРСОС

2. В системе GPS кодировка сигналов основана на ЛРСОС. В стартовом режиме приемник выполняет позиционирование в интервале от 97531мс до 131706 мс при мощности навигационного сигнала от -50 дБм до -80 дБм. Для более быстрого позиционирования и улучшения GPS приемника можно выделить два главных метода оптимизации приемника:

- повышение корреляционных и автокорреляционных свойств псевдослучайных последовательностей;
- повышение скорости генерации локальных псевдослучайных последовательностей путем параллелизации.

Все исследования и результаты диссертационной работы направлены на решение вышеперечисленных задач.

Во второй главе рассматривается генератор псевдослучайных последовательностей С/А кодов, а также исследуются методы корреляции для обнаружения сигнала. На основе результатов исследования были разработаны программные пакеты для генерации псевдослучайных последовательностей С/А кодов по данному номеру спутника и для корреляции кодированных навигационных сигналов.

1. Последовательности С/А кодов относятся к семейству псевдослучайных последовательностей. Генератор С/А кодов основан на двух линейных регистрах сдвига Фибоначчи, которые работают на тактовой частоте 1023 МГц (рис.1). Каждый из регистров состоит из десяти битов, которые поочередно связаны между собой. Те биты, которые соединены с входом первого бита, называются обратными связями регистра. Характеристики выходных последовательностей зависят от количества битов и обратных связей регистра.

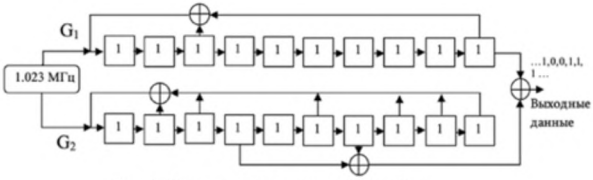


Рис.1.Схема генератора С/А кодов

Как показана на рис.1, биты обратных связей для первого регистра G_1 находятся на позициях 3 и 10, а для второго регистра G_2, - на позициях 2, 3, 6, 8, 9, 10. Выходные данные от регистров G_1 и G_2 суммируются по модулю. Для G_1 берутся последовательности из десятого регистра, что является стандартом для каждого спутника при генерации С/А кодов. Для регистра G_2 берутся выходные данные из двух регистров (выбранных по номеру спутника из таблицы Роберта Голда), которые складываются по модулю два, после чего суммируются с последовательностями из регистра G_1. Этот подход применяется при генерации С/А кодов для каждого спутника, что позволяет сгенерировать уникальные псевдослучайные последовательности для каждого спутника.

2. На основе результатов исследования генератора С/А кодов разработана графическая программа, которая позволяет сгенерировать С/А последовательности по выбранному номеру спутника (рис.2).

3. В навигационной системе GPS широко используются два вида корреляции сигналов: взаимная и круговая, в основе которых лежат уравнения для общей корреляции.

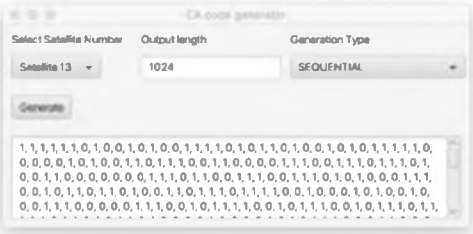


Рис.2. Графическая программа для генерации С/А последовательностей

Для данных цифровых сигналов $X(n) = \{X_1, X_2, X_3, X_4, \ldots, X_N\}$ и $Y(n) = \{Y_1, Y_2, Y_3, Y_4, \ldots, Y_N\}$ общее уравнение корреляции можно описать в виде где **n** - относительная позиция между сигналами X и Y, а $X(n)$ и $Y(n)$ - амплитуды сигналов в позиции **n**.

$$\text{Corrxy} = \sum_{n=0}^{N} \frac{X(n)Y(n)}{\sqrt{\sum_{n=0}^{N} X^2(n) \sum_{n=0}^{N} Y^2(n)}}, \qquad (1)$$

Таблица. Матрица корреляции для сигналов X и Y

	Y(-n)	N	4	3	2	1
X(n)		Y_N	Y_4	Y_3	Y_2	Y_1
1	X_1	$X_1 Y_N$	$X_1 Y_4$	$X_1 Y_3$	$X_1 Y_2$	$X_1 Y_1$
2	X_2	$X_2 Y_N$	$X_2 Y_4$	$X_2 Y_3$	$X_2 Y_2$	$X_2 Y_1$
3	X_3	$X_3 Y_N$	$X_3 Y_4$	$X_3 Y_3$	$X_3 Y_2$	$X_3 Y_1$
4	X_4	$X_4 Y_N$	$X_4 Y_4$	$X_4 Y_3$	$X_4 Y_2$	$X_4 Y_1$
N	X_N	$X_N Y_N$	$X_N Y_4$	$X_N Y_3$	$X_N Y_2$	$X_N Y_1$

С целью получения алгоритма расчета корреляционного коэффициента для данных двух цифровых сигналов X и Y, приведем двумерную матрицу, содержащую амплитуды сигналов $X(n)$ и $Y(-n)$, где $Y(-n)$ –реверсный массив амплитуд сигнала $Y(n)$ (см.табл.).

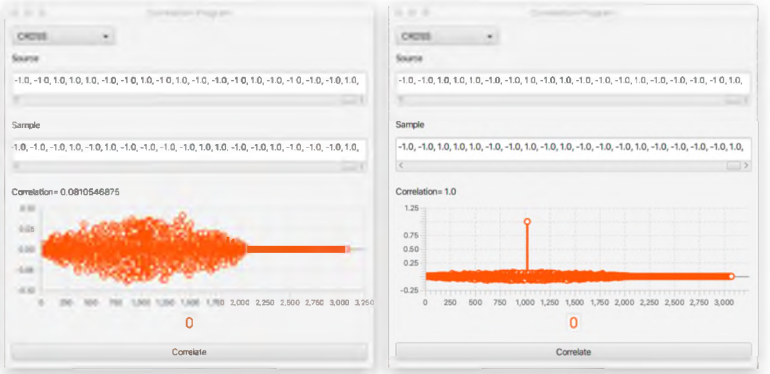
Как видно из таблицы, первый столбец матрицы состоит из массива амплитуд сигнала X, а первая строка - из реверсного массива амплитуд Y. Остальные строки матрицы получаются умножением значений амплитуд $X(n)$ в столбце на значения амплитуд $Y(-n)$. Коэффициент корреляции выражается суммой умноженных значений матрицы по диагонали:

$$\begin{aligned}
&Corr_{xy}[1] = X_1Y_n \\
&Corr_{xy}[2] = X_2Y_n + X_1Y_{n-1} \\
&Corr_{xy}[3] = X_3Y_n + X_2Y_{n-1} + X_1Y_{n-3} \\
&\ldots \\
&Corr_{xy}[n] = X_1Y_1 + X_2Y_2 + X_3Y_3 + \ldots . X_nY_n \\
&Corr_{xy}[n+1] = X_2Y_1 + X_3Y_2 + \ldots + X_{n-1}Y_{n-2} + X_nY_{n-1} \\
&\ldots \\
&Corr_{xy}[2n-1] = X_nY_1.
\end{aligned} \qquad (2)$$

При сумме значений из (2) получается корреляционный коэффициент двух сигналов, который делится на коэффициент нормализации (3), для получения значения в диапазоне [-1,1].

$$norm = \sqrt{\sum_{n=0}^{N} X^2(n) \sum_{n=0}^{N} Y^2(n)} \tag{3}$$

4. Базируясь на данной методике вычисления корреляционного коэффициента, разработаны алгоритмы для выполнения взаимной и циркулярной корреляций цифровых сигналов, работа которых подтверждается разработанной программой в среде «Java». Программа вычисляет максимальный пик корреляции для данных двух цифровых сигналов, используя алгоритмы взаимной и циркулярной корреляций. На рис.3 показана графическая программа для вычисления взаимной корреляции между двумя последовательностями С/А кодов для первого и второго спутников, которая составляет $Corr_{xy}=0.081$ (рис.3а), и автокорреляции С/А кода для первого спутника (рис.3б).



а) *б)*

Рис.3. Графическая программа для вычисления корреляции(а) и автокорреляции (б) между двумя цифровыми сигналами

Данная программа корреляции используется в работе для дальнейшего исследования С/А кодов.

<u>В третьей главе</u> исследуются методы повышения корреляционных свойств С/А кода, являющиеся одним из наиболее оптимальных методов. В главе рассматриваются последовательности с максимальными

корреляционными свойствами, которые сравниваются со свойствами С/А кодов. Это дает понять насколько можно улучшить корреляционные свойства С/А кодов. Для генерации последовательностей с максимально высокими корреляционными свойствами используются генетические алгоритмы, которые предназначены для решения задач оптимизации.

1. Работа генетических алгоритмов основана на идее естественного отбора. Для реализации решения задачи с помощью генетических алгоритмов сначала следует определить значения базовых элементов, составляющих алгоритм. К ним относятся:

Популяция – описывает группу индивидуумов или массив решений для данной задачи. Каждый из индивидуумов включает в себя ген и коэффициент эффективности. Ген описывает определенное решение для данной задачи и часто представляется двоичным кодом. Коэффициент эффективности выражает эффективность решения задачи или же эффективность гена.

Мутация – оператор алгоритма, который случайным образом меняет ген выбранного индивидуума.

Скрещивание – оператор алгоритма, который применяется для скрещивания двух индивидуумов, в результате чего получается новый индивидуум, ген которого наследует общие черты родителей.

Выбор родителей – оператор алгоритма, который применяется для выявления индивидуумов с высокими коэффициентами эффективности с целью дальнейшей мутации и скрещивания.

Условия прекращения генерации - условия для остановки генерации алгоритма при нахождении решения для задачи.

На рис.4 показана общая диаграмма работы генетического алгоритма.

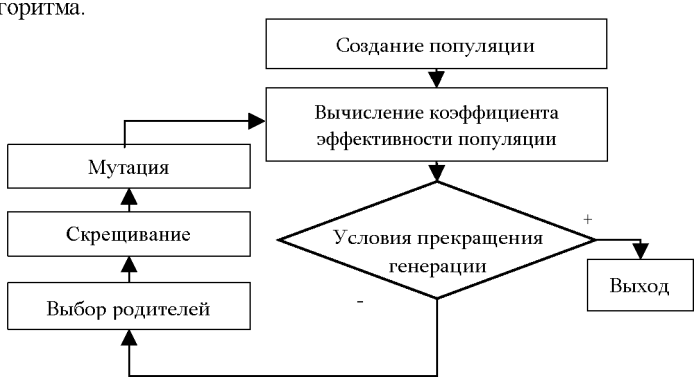


Рис.4. Общая диаграмма работы генетического

Как видно из рис.4, сначала генерируется новое поколение на основе случайных последовательностей. После создания начальной генерации вычисляется коэффициент эффективности каждого индивидуума. Следующим шагом проверяется условие прекращения генерации, которое с первого раза обычно не бывает положительным. При отрицательном результате проверки коэффициента эффективности применяются операторы скрещивания и мутации на выбранных индивидуумах из текущей популяции, после чего цикл генерации повторяется.

2. Рассматривается модель индивидуума для случайных последовательностей и вычислен их коэффициент эффективности. Ген индивидуума является массивом длиной 32*1023 бита (32 - количество спутников, а 1023 - цикл повторения С/А последовательностей для каждого спутника). Из массива гена индивидуума первые 0-1022 бита относятся к первому спутнику, следующий интервал битов от 1023 до 2046 - ко второму спутнику и т.д. Диаграмма вычисления коэффициента корреляции для индивидуума показана на рис.5.

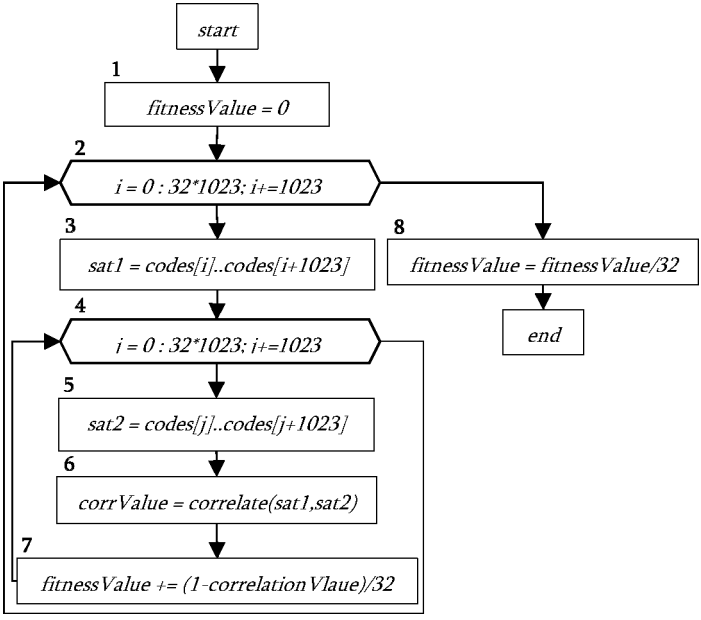


Рис.5. Диаграмма вычисления коэффициента эффективности для индивидуума случайных последовательностей

Процесс вычисления коэффициента эффективности основан на двух итерациях для каждого диапазона последовательностей спутника. На первом шаге значение коэффициента эффективности приравнивается нулю. После начинается первая итерация, где из гена индивидуума выбирается первый диапазон кодов длиной 1023 бита, который присваивается *sat1*. На следующем шаге начинается вторая итерация по диапазонам последовательностей спутников. По номеру итерации выбирается второй диапазон кодов, который присваивается *sat2*. Следующим шагом является вычисление коэффициента корреляции для выбранных двух последовательностей *sat1* и *sat2*. Так как алгоритм должен искать последовательности, которые максимально отличаются друг от друга, берется реверсное значение полученного коэффициента корреляции для добавления к коэффициенту эффективности. Для нормализации конечного коэффициента эффективности его значение делится на 32 в конце первой итерации и при каждом цикле второй итерации. После вычисления значения коэффициента эффективности получаются в диапазоне от -1 до +1, где значение +1 указывает на максимально разные последовательности.

Для случайных последовательностей при определении условия прекращения генерации вместо номинального значения выбирается техника, при которой работа алгоритма продолжается до тех пор, пока в предстоящих *n* шагах генерации не наблюдается роста коэффициента эффективности.

Для мутации и скрещивания выбор индивидуумов случайных последовательностей выполняется с помощью алгоритма выбора “Рулетки”, где с большой вероятностью выбираются индивидуумы с высокими значениями коэффициента эффективности.

Для контроля количества скрещиваний и мутаций индивидуумов в алгоритм вводятся коэффициенты частот скрещивания и мутаций. Генетический алгоритм будет неэффективным, если применить скрещивания и мутацию для всех индивидуумов в популяции, поскольку индивидуумы будут слишком быстро меняться.

Для сохранения лучших индивидуумов в популяции в алгоритм было введено значение количества элиты, с помощью которого индивидуумы с высокими коэффициентами эффективности, обходя шаги мутации и скрещивания, попадают из старого поколения в новое.

3. Базируясь на алгоритме генерации случайных последовательностей, в работе разработана программа, которая дает возможность сгенерировать последовательности с максимальными высокими корреляционными свойствами по отношении друг к другу (рис.6).

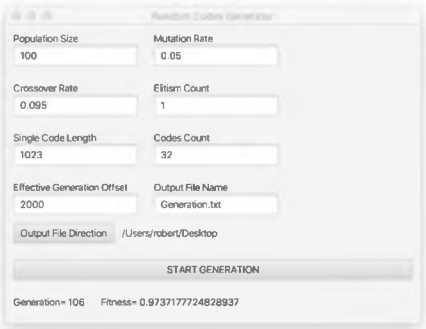
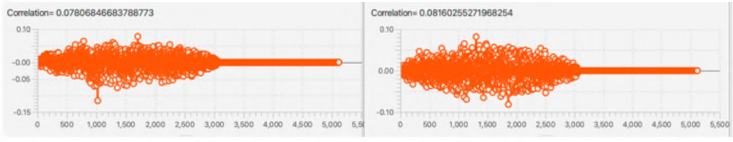


Рис.6. Генератор случайных последовательностей

Программа допускает генерацию последовательности любой длины и количества. Для генерации последовательностей, похожих на последовательности C/A кодов, в окно программы вводятся длина кода 1023 (один цикл повторения) и количество кодов 32 (количество спутников). После генерации программа записывает выходные последовательности в файле. Корреляционные свойства полученных последовательностей проверяются в программе корреляции. Коэффициент взаимной корреляции для двух выбранных последовательностей составляет $Corr_{xy}= 0,078$ (рис.7а). Для сравнения полученных результатов с корреляционными свойствами C/A кодов выбраны последовательности для спутников под номерами 13 и 15, где коэффициент корреляции составляет $Corr_{xy}= 0,081$ (рис.7б).



а) б)

Рис.7. Корреляция между случайными (а) и C/A последовательностями (б)

Аналогичные результаты получаются для корреляционных свойств между другими комбинациями спутников и последовательностей случайных чисел, из чего следует, что корреляционные свойства последовательностей C/A кодов находятся на максимальном уровне и не подлежат дальнейшему повышению.

В четвертой главе рассматриваются методы быстрой генерации псевдослучайных последовательностей как для ЛРСОС, так и для генератора C/A кодов. Так как генерация псевдослучайных

последовательностей является линейным и последовательным процессом, к ней применяется подход параллелизации.

1. Выводятся формулы для ЛРСОС, которые выражают связь между шагом генерации и состоянием регистра, где состояние регистра определяется значениями битов на данном шаге генерации. Для регистра Фибоначчи с длиной **n** битов и с обратными связями в позициях l_k связь между состояниями битов S и шагами генерации i показана с помощью следующего уравнения:

$$S_{i+n} = \oplus \sum_{l} S_{i+(n-l)} \tag{4}$$

Аналогичная связь существует и для линейного регистра Галуа, которая имеет вид

$$S_{i+n} = S_i + \oplus \sum_{l} S_{i+(l-1)} \tag{5}$$

Используя уравнения (4) и (5), с помощью уже сгенерированных состояний регистра можно определить предстоящие состояния, что важно для алгоритма параллелизации регистра.

2. Разработанный алгоритм для параллельной генерации выходных данных ЛРСОС основан на уравнениях (4) и (5). Для данного регистра процесс параллельной генерации выходных данных абстрактно показан на рис.8, где для генерации выходных данных используется более чем один регистр.

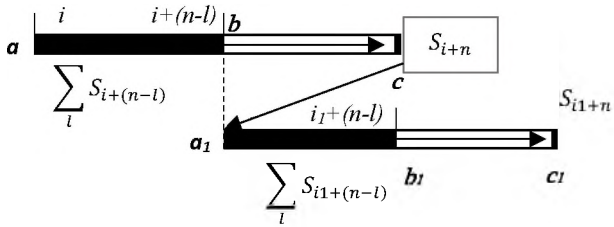


Рис.8. Абстрактное представление процесса параллелизации линейного регистра сдвига с обратной связью

Начинает генерацию первый регистр. Доходя до точки b, имея все необходимые состояния, вычисляются значения битов для предстоящего шага генерации $i+n$. Вычисленные значения битов для S_{i+n} состояния регистра присваиваются битам второго регистра как начальное состояние. Далее второй регистр параллельно с первым регистром начинает новый этап генерации выходных битов. Аналогичный процесс повторяется для второго

регистра, который, дойдя до своей точки параллелизации b_1, вычисляет предыдущие биты и присваивает их битам следующего регистра. Значения шагов параллелизации для регистра Фибоначчи вычисляются с помощью следующего уравнения:

$$i_p = n * p + (n - l)\ , \qquad \text{где } p \in N, 0 \le p \le (2^n - 1)/n). \tag{6}$$

Для регистра Галуа имеем аналогичное уравнение

$$i_p = n * p + (l - 1), \qquad \text{где } p \in N, 0 \le p \le (2^n - 1)/n). \tag{7}$$

Связь между параметрами и количеством используемых линейных регистров Фибоначчи для параллельной генерации выходных последовательностей имеет вид

$$N_{GF} = \left[\frac{n}{n - l_f}\right] + 1. \tag{8}$$

Для регистра Галуа имеем аналогичное уравнение

$$N_{GG} = \left[\frac{n}{l_l - 1}\right] + 1 \tag{9}$$

В работе также получена связь между параметрами регистра и соотношениями продолжительностей параллельной и последовательной генерации последовательностей в виде

$$\frac{T_S}{T_P} = \frac{n2^{n-1}}{l2^{n-1} + n^2 - nl}, \tag{10}$$

где T_S - продолжительность последовательной генерации; T_P - продолжительность параллельной генерации; l - номер первой точки параллелизации.

Для регистра Фибоначчи $l = (n\text{-}l_k)$, где l_k - номер первого бита обратной связи регистра. Для регистра Галуа $l = (l_k\text{-}1)$, где l_k - номер последнего бита обратной связи регистра.

Значения соотношения продолжительностей параллельной и последовательной генерации для кодов C/A составляют 1,28, для CMCL - 1,17, а для I5 Q5 -1,18.

Основываясь на выражениях алгоритма параллельной генерации выходных данных ЛРСОС, была разработана программа в среде “Java”, с помощью которой, вводя позиции обратной связи, длину и тип регистра, можно последовательно и параллельно сгенерировать выходные последовательности (рис.9). На базе на данного программного кода была

реализована программа параллельного генератора С/А кодов (рис.2), где для выполнения параллельной генерации в поле “Generation Type” следует выбрать вариант “PARRALLEL”

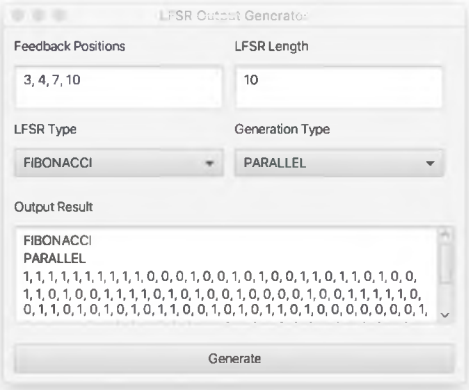


Рис.9. Программа для генерации выходных данных регистров Фибоначчи и Галуа параллельным и последовательным методами

3. На основе параллельной генерации С/А кодов можно реализовать общую параллельную генерацию С/А последовательностей для всех спутников одновременно. Абстрактная структура такого генератора (рис.10) состоит из обычного тактового генератора частотой 1,023 МГц, подключенного к двум параллельным ЛРСОС.

Для каждого спутника к определенным битам регистра (таблица Роберта Голда) G_{P2} подключены фазовые селекторы. Во время генерации последовательностей G_{P2}, фазовые селекторы выбирают именно те биты, которые указаны для данного спутника.

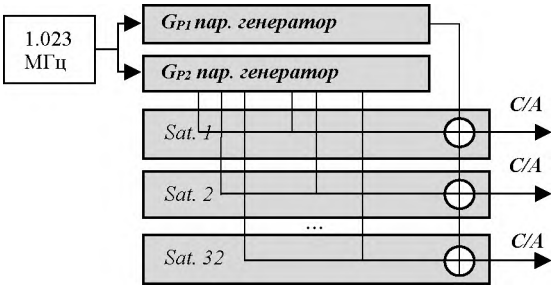
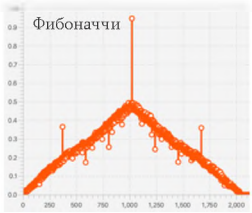


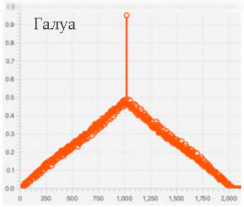
Рис.10. Общая параллельная генерация С/А кодов

4. Пользуясь методом параллельной генерации последовательностей ЛРСОС, разработан метод генерации прерывающихся последовательностей. Основной принцип этого метода состоит в том, что при генерации выходных последовательностей применяется метод параллельной генерации, однако биты из интервалов параллелизации не генерируются, тем самым ускоряя общий процесс генерации. В результате среднее значение пика корреляции незначительно уменьшается, но остается пригодным для обнаружения сигнала. Метод генерации прерывающихся последовательностей дает возможность быстро сгенерировать выходные последовательности с помощью одного регистра, при этом сохраняя их корреляционные свойства. С целью изучения корреляционных свойств прерывающихся последовательностей для регистров Фибоначчи, Галуа и генератора С/А рассматривается значение корреляционных пиков между оригинальным сигналом и его прерывающей версией последовательностей (рис.11).

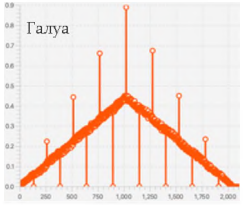
Обр. связь { 3, 5, 8, 10}
$Corr_{xy}$ = 0.907



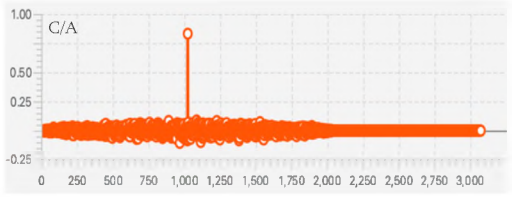
Обр. связь { 2, 4, 6, 7, 9, 10 }
$Corr_{xy}$ = 0.947



Обр. связь { 2, 7, 9 }
$Corr_{xy}$ = 0.949



Обр. связь { 2, 8 }
$Corr_{xy}$ = 0.889



Номер спутника 19.
$Corr_{xy}$ = 0.831

Рис.11. Корреляционные пики между оригинальным сигналом и его прерывающейся версией для регистров Фибоначчи, Галуа и генератора С/А

Как видно из рис.11, взаимно корреляционный пик между оригинальным сигналом и его прерывающейся версией выделяется на графике, что дает возможность применения метода прерывающейся генерации псевдослучайных последовательностей при проектировании приемников навигационной системы.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Исследованы сигналы старого и нового поколений навигационной системы GPS и вычислено среднее время для позиционирования приемника [1].

2. На основе конструкций генераторов псевдослучайных последовательностей C/A кодов и работы линейных регистров с обратной связью разработаны программные модели ЛРСОС Фибоначчи и Галуа, с помощью которых создана программа генерации C/A последовательностей для заданной длины и спутника. Исследования видов взаимной и циркулярной корреляции сигналов позволили разработать программу, позволяющую получить график их корреляции и вычислить коэффициент корреляции между двумя сигналами [2,3].

3. На основе генетических алгоритмов разработана программа, позволяющая сгенерировать случайные последовательности с высокими корреляционными свойствами (***$Corr_{xy}$=0.07…0.08***) для заданного количества *n* и длины *l*. Проведены сравнения корреляционных свойств между последовательностями, генерированными генетическими алгоритмами, и последовательностями C/A кодов [4].

4. На основе результатов исследования последовательности регистров Фибоначчи и Галуа выведены два выражения для регистров, которые описывают связь между шагами генерации и значениями битов регистра [5].

5. Базируясь на выражениях соотношения шага генерации и состояния регистра, разработаны методы параллелизации регистров Фибоначчи и Галуа, которые сокращают время генерации выходных последовательностей для одного цикла повторения. Вычислена связь между соотношениями продолжительностей параллельной и последовательной генерации выходных данных и параметрами регистра. Для генератора C/A кодов соотношение между длительностями поочередной и параллельной генерации составляет ***1,28***, что дает сокращение во времени позиционирования ***21334…28810 мс*** при мощности сигнала от -50 дБм до -80 дБм. Для CMCL кодов это соотношение составляет ***1,17***, что дает сокращение во времени позиционирования ***14171…19136 мс***, а для I5 и Q5 кодов - ***1,18*** и сокращает время позиционирования от ***14877 мс*** до ***20090 мс***. Также приведена связь между параметрами и количеством используемых ЛРСОС для аппаратной реализации метода параллельной генерации выходных последовательностей [5,6].

6. Разработан алгоритм параллельной генерации последовательностей C/A кодов на основе параллельных регистров Фибоначчи, работа которого проверена в программной среде [7].

7. На основе полученных выражений, иллюстрирующих связь между шагами генерации и значениями битов ЛРСОС, разработан метод генерации прерывающихся последовательностей, который позволяет осуществить более быструю генерацию выходных последовательностей. Выполнено сравнение корреляционных связей между генерированными прерывающимися и непрерывающимися последовательностями C/A кодов.

Основные результаты диссертации опубликованы в следующих работах:

1. Ապիկյան Ռ. Կ. Արբանյակային ռադիոնավիգացիոն համակարգի, ընդունիչի զգայունության թեստավորումը// ՀԱՊՀ Լրաբեր. Գիտական հոդվածների ժողովածու. - Երևան: Ճարտարագետ, 2017. - մաս 1. - էջ 447-451:
2. Ապիկյան Ռ. Կ. Արբանյակային ռադիոնավիգացիոն համակարգի՝ C/A կոդով նավիգացիոն տվյալների մոդուլացման և ապամոդուլացման սեգմենտի մշակումն ու մոդելավորումը Java միջավայրում// ՀԱՊՀ Լրաբեր. Գիտական հոդվածների ժողովածու. - Երևան: Ճարտարագետ, 2018. - մաս 1. - էջ 309-316:
3. Gomtsyan H.A., Apikyan R.K. Building GPS Receiver's correlation functions with Kotlin programming language// Banber, proceedings of NPUA, Yerevan 2019. -vol. 2. -no. 2, -pp. 109-119.
4. Gomtsyan H., Apikyan R. Code Sequence Generation with Genetic Algorithms, with Correlation Properties Similar to GPS C/A Codes// Computer Science and Information Technologies (CSIT) 2019. -pp. 127-129.
5. Gomtsyan H., Apikyan R., Bayadyan V. Double Feedback LFSR Parallel Output Generation// International Journal of Sciences: Basic and Applied Research (IJSBAR) 2019. -vol. 48. -no. 3. -pp. 143-149.
6. Гомцян О., Апикян Р. Вычисление и измерение разницы времен при параллельной и последовательной генерации кодов C/A, CM И CL для GPS Спутника// Век качества, Москва 2020. -но. 1. -с. 158-169.
7. Apikyan R. K. GPS satellites parallel C/A code generation// Proceedings of NAS RA and NPUA. Series of Technical Sciences 2019. -vol. 72. -no. 4. -pp. 520-524.

ԱՄՓՈՓԱԳԻՐ

Արբանյակային ռադիոնավիգացիոն համակարգերում ազդանշանները մոդուլվում են քվազիպատահական կոդերի հաջորդականություններով, որի արդյունքում հաղորդված ազդանշանը դառնում է ավելի աղմկակայուն, իսկ

պարունակող արբանյակային ինֆորմացիան՝ ավելի պաշտպանված: Չնայած՝ քվազիպատահական հաջորդականություններով ազդանշանի մոդուլումը տալիս է մի շարք առավելություններ, ընդունիչի տեսանկյունից այն պահանջում է հավելյալ ժամանակ՝ ազդանշանի հայտնաբերման և դեկոդավորման համար, քանի որ մինչ ազդանշանի հայտնաբերմանն անցնելը իրականացվում է քվազիպատահական հաջորդականությունների տեղային գեներացում, որից հետո իրականացվում է կոռելյացիա ընդունիչի ալեհավաքի մոտ տարբեր արբանյակներից հաղորդած ազդանշանների գումարային դաշտի և տեղային գեներացված հաջորդականությունների միջև: Ընդունիչով իրականացվող հաջորդականությունների տեղային գեներացիայի ժամանակի կրճատման պարագայում, հնարավոր է տեղորոշումն իրականացնել ավելի արագ :

1. Հետազոտվել են GPS համակարգի նախնական և ժամանակակից ազդանշանների տեսակները և ազդանշանի հայտնաբերման միջին տևողությունը:

2. Ծրագրային միջավայրում մշակվել են Ֆիբոնաչիի և Գալուայի ԳՀԿՏՌ-ների ռեգիստրների մոդելները, որոնց հիման վրա մշակվում է C/A կոդի գեներացիայի ծրագիր, որով հնարավոր է իրականացնել քվազիպատահական կոդերի գեներացում, ըստ տրված արբանյակի համարի և երկարության: GPS ռադիոնավիգացիոն համակարգում ընդունիչի կողմից կիրառվող ազդանշանների կոռելյացիայի տեսակների հետազոտության հիման վրա մշակվում է ծրագիր, որը հնարավորություն է տալիս հաշվարկել ներմուծած ազդանշանների կոռելյացիայի արժեքները և կառուցել ստացված կոռելյացիայի արժեքներին համապատասխան գրաֆիկը:

3. Գենետիկ ալգորիթմների հիման վրա մշակվել է պատահական կոդերի գեներատոր, որով կարելի է գեներացնել թվով n և l երկարությամբ՝ միմյանց նկատմամբ բարձր կոռելյացիոն հատկություններով օժտված հաջորդականություններ: Իրականացվում է գենետիկ ալգորիթմներով գեներացված պատահական հաջորդականությունների և C/A կոդի հաջորդականությունների կոռելյացիոն հատկությունների համեմատություն:

4. Ծրագրային միջավայրում հետազոտվել են Ֆիբոնաչիի և Գալուայի ռեգիստրների գեներացման քայլերի և բիտերի արժեքների միջև կապերը: Հետազոտության արդյունքում դուրս է բերվել երկու արտահայտություն Ֆիբոնաչիի և Գալուայի ռեգիստրների համար, որոնք բնութագրում են ռեգիստների գեներացիայի քայլին համապատասխան բիտերի արժեքների միջև կապը:

5. Ստացված բանաձևերի հիման վրա մշակվել են Ֆիբոնաչիի և Գալուայի ռեգիստրների զուգահեռացման եղանակներ, որոնք հնարավորություն են տալիս կրճատել գեներացիայի տևողությունը ելքային հաջորդականությունների

կրկնման մեկ ցիկլի համար: Ըստ ռեգիստրի պարամետրերի՝ հաշվարկվել է զուգահեռ և հաջորդական գեներացիաների համար պահանջվող ժամանակատվածների հարաբերակցությունը: Նավիգացիոն ազդանշանի -50 դԲմ-ից -80 դԲմ առկայության դեպքում հաշվարկվում է C/A, CL CM, I5 Q5 հաջորդականությունների զուգահեռ գեներացիայի արագագործությունը հաջորդական գեներացիայի նկատմամբ, որի արդյունքում C/A կողի համար՝ ստացվում է ***1,28*** անգամ գեներացիայի գործընթացի արագացում և ***21334…28810 մվ***-ով տեղորոշման ժամանակի կրճատում, CL CM կողերի համար՝ ***1,17*** անգամ արագացում և ***14171…19136 մվ*** տեղորոշման ժամանակի կրճատում, իսկ I5 Q5 կողերի համար ***1,18*** անգամ արագացում և ***14877 մվ-ից*** մինչև ***20090 մվ*** տեղորոշման ժամանակի կրճատում: Ինչպես նաև դուրս է բերվել զուգահեռ գեներացիայի իրականացման համար պահանջվող ռեգիստրների քանակի և ռեգիստրի պարամետրերի միջև կապը:

6. Ստացված Ֆիբոնաչիի զուգահեռ ռեգիստրի հիման վրա մշակվել է C/A կողի ելքային հաջորդականությունների զուգահեռ գեներացիայի մեթոդը, որի աշխատանքը ստուգվում է ծրագրային միջավայրում:

7. Հիմք ընդունելով ռեգիստրների գեներացիայի քայլին համապատասխան բիտերի արժեքների միջև կապը նկարագրող արտահայտությունները՝ մշակվել է ելքային հաջորդականությունների ընդհատումներով գեներացման եղանակը, որը հնարավորություն է տալիս ավելի արագ իրականացնել ելքային հաջորդականությունների գեներացում, օգտագործելով թվով մեկ ԳՀԿՏՈ: Իրականացվում է կոռելյացիոն հատկությունների ստուգում ընդհատումներով և անընդհատ C/A հաջորդականությունների միջև:

Robert Apikyan

DEVELOPMENT AND RESEARCH OF EFFECTIVE GPS ENCRYPTION ALGORITHMS

SUMMARY

In the satellite radio navigation system, signals are modulated with pseudo-random numbers (PRN), which encrypts the navigation information and make the transmitted signal more resistant to noises. Although the advantages of signal modulation with PRN numbers, from the receiver side it will require additional time for signal acquisition and information decoding, as it will first locally generate the PRN sequences and then perform a correlation between the

generated sequences and the summary signal near the receiver's antenna. It's possible to rich fast positioning by the receiver in case of shorting the required time for PRN generation.

1. Signal and information encryption are being studded used by the Global Positioning System.

2. The models of Fibonacci and Galois LFSR's are developed in the software environment and based on that was developed the C/A code generator, which allows the generation of the PRN sequences for the given length and number of the satellite. Based on studies of correlation types used by the GPS system, the program was developed, which allows calculating the cross and circular correlation values for given signals and chart a correlation graph for them.

3. A random code generator is developed based on genetic algorithms, which allows the generation of sequences for length n ы 1. Was performed a comparison of correlation properties between the random sequences generated by genetic algorithms and PRN code sequences generated by the C / A code generator.

4. In the software environment, the path between tabs and the generation step is examined for Fibonacci and Galois LFSR types. As a result of the research, two expressions are taken out for Fibonacci and Galois LFSRs, that describes the path between the generation step and the tabs values of register.

5. Based on the obtained expressions, methods of parallelization are developed for Fibonacci and Galois register types, which allow reducing the required generation time for one cycle of repetition of output sequences. Depending on the parameters of the register, the ratio between the required time for parallel and linear generations is calculated, for C/A code sequences its equal to ***1,28*** and reduce the acquisition time by ***21334…28810 ms***, for CL CM sequences its equal to ***1,17*** and reduce the acquisition time by ***14171…19136 ms***, for I5 and Q5 codes its equal to ***1,18***, which reduce the acquisition time by ***14877…20090 ms,*** where the power of the received signal is between -50 dBm and -80 dBm. As well as the expression is taking out, which describes the path between the parameters of register and the required registers count, for parallel output generation, in hardware schemas.

6. The method of parallel generation for C/A output sequences is developed, based on the method of parallel output generation for Fibonacci's LFSR and examined in the software environment

7. Based on the expressions that describe the path between register's the generation step and tabs values, the partial generation method is developed for output sequences, which allows making fast generation of the output sequences by using only one LFSR. The correlation properties analysis is performed between partially and fully generated codes.