УДК 004.056.55

Ушакова А.А.,
студент МГТУ им. Н.Э. Баумана факультета
«Информатика и системы управления»,
кафедры «Защита информации»,
Россия, 105005, г. Москва
Борукаева А.О.,
студент МГТУ им. Н.Э. Баумана факультета
«Информатика и системы управления»,
кафедры «Защита информации», сотрудник регионального учебно-научного
центра «Безопасность» МГТУ им. Н.Э. Баумана,
Россия, 105005, г. Москва
Бердиков П.Г.,
студент МГТУ им. Н.Э. Баумана факультета
«Информатика и системы управления»,
кафедры «Защита информации»,
Россия, 105005, г. Москва
Научный руководитель: Филатов В.И.

ИССЛЕДОВАНИЕ КОРРЕЛЯЦИОННЫХ ХАРАКТЕРИСТИК СЕМЕЙСТВ КОДОВ РАЗНЫХ ДЛИН

Аннотация: *В данной статье рассмотрено применение полиномов Лежандра в различных технических науках. Построен генератор последовательности Лежандра на языке программирования Matlab. Произведены расчеты автокорреляционной функции и взаимокорреляционной функции с различной длинной полинома и построены их графики в среде Matlab. Проведен расчет арсенальной скрытности и анализ выбранных кодов согласно методики Л. Каневского. Сделаны выводы о структуре кодовых последовательностей и об их арсенальной скрытности.*

Ключевые слова: *Полином Лежандра, взаимокорреляционная функция, автокорреляционная функция, арсенальная скрытность.*

Annotation: *This article discusses the use of Legendre polynomials in various technical sciences. Legendre sequence generator built on the programming language Matlab. Calculations of the autocorrelation function and the interrelation functions with different lengths of the polynomial and construct their graphs in Matlab environment. Calculation signal hiding and analysis of selected codes according L. Kanevskogo techniques. The conclusions about the structure of the code sequences and their signal hiding.*

Key words: *Legendre multinomial, cross-correlation function, autocorrelation function, signal hiding.*

Введение

Статья посвящена исследованию возможностей применения полиномов Лежандра в физике для исследования полей: построен генератор последовательности Лежандра на языке программирования Matlab, произведены расчеты, сделаны выводы о структуре кодовых последовательностей и об их арсенальной скрытности.

Статья актуальна, поскольку бинарные последовательности Лежандра, формируемые на основе двузначного характера, широко применяются в физике, в том числе для мультипольного разложения электростатических полей и расписание полей на парциальные волны.

В статье приведен способ построения генератора последовательности Лежандра на языке программирования Matlab. Произведены расчеты автокорреляционной взаимокорреляционной функций с различной длинной полинома и построены их графики в среде Matlab. Выполнен расчет арсенальной скрытности и анализ выбранных кодов согласно методики Л.Каневского. Сделаны выводы о том, что с увеличением длины полинома Лежандра арсенальная скрытность увеличивается.

Теория

1 способ

Бинарные последовательности Лежандра формируются на основе двузначного характера. Возьмем простое p и построим простое поле GF(p). Отождествим его элементы (0, 1, … , p-1) с номерами позиций i символов a_i периодической бинарной последовательности $\{a_i\}$ периода p. Тогда для периодической версии последовательности Лежандра правило формирования определяется в виде:

$$a_i \begin{cases} +1, & \mathrm{i} = 0 \mathrm{mod} \mathrm{p} \\ \psi(\mathrm{i}), & \mathrm{i} \neq 0 \mathrm{mod} \mathrm{p} \end{cases}$$

Двузначным характером (символом Лежандра) ψ(a) ненулевого элемента, а поля GF(p), где p – некоторое натуральное число, называется функция, принимающая значения +1 и -1 в зависимости от честности или нечетности логарифма [1].

2 способ

Полином Лежандра определяется формулой:

$$P(n,x) = \frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2-1)^n$$

$$P(n,x) = \frac{2n-1}{n}xP(n-1,x) - \frac{n-1}{n}P(n-2,x), \text{где } P(0,x) = 1, P(1,x) = x$$

Полиномы Лежандра ортогональны на отрезке [-1, 1] с весовой функцией w(x)=1.

Применение

I. Полиномы Лежандра широко применяются **в физике**. Обычно аргументом полиномов является косинус полярного угла θ, Который изменяется от -1 при $\theta = \pi$ к 1 при $\theta = 0$.

В частности, для получения **мультипольного разложения электростатических полей:**

$$\frac{1}{|r - r_0|} = \frac{1}{\sqrt{r^2 - 2rr_0\cos\theta + r_0^2}} = \frac{1}{r_0}\frac{1}{\sqrt{1 - 2x\cos\theta + x^2}} = \frac{1}{r_0}\sum_n P_n(\cos\theta)x^n$$

где $x = r/r_0$, А $\cos\theta$- Угол между векторами $\mathbf{r}$ и $\mathbf{r}_0$.

Другое важное применение - **расписание полей на парциальные волны** [2]**.** Например, плоская волна раскладывается с помощью формулы

$$e^{ik\cdot r} = \sum_{l=0}^{\infty}(2l+1)i^l j_l(kr)P_l(\cos\theta)$$

где $j_l(x)$ - сферические функции Бесселя.

II. Использование свойств полинома, который был образован из полинома Лежандра и максимально плоского полинома, может улучшить качество аппроксимации при решении задач построения электрических фильтров и согласующих цепей по одному из критериев [3].

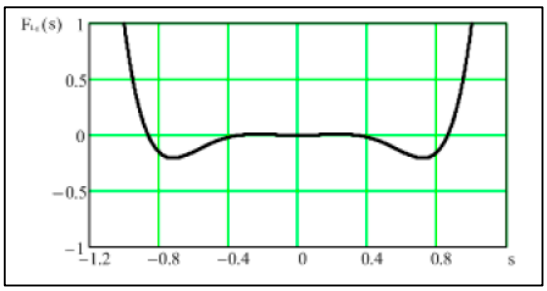

Рис. 1. Вид модифицированного полинома Лежандра

Листинг (создание генератора полиномов Лежандра [4-8])

Рассмотрим создание полиномов Лежандра, для полноты картины и приятного восприятия, указываются пояснения. Данный способ позволяет проанализировать его наглядность и понятный механизм построения. В дальнейшем будет проведен анализ скрытности данных.

```
%% Генератор полиномов Лежандра
```

```
clear;
close all;
 % способ 1 (через встроенную функцию)
n=randi(10); %n - максимальная степень полинома (возмож
от 1 до 10)
syms x; %x - основание полинома
for i=1:1:n
    a(i)=legendreP(i,x); %i - сетепнь полинома, x -
основание
end
disp(a);

% способ 2 (вручную)
%n=randi(10); %n - максимальная степень полинома (возмож
от 1 до 10)
syms x; %x - основание полинома
for i=1:1:n
    d=diff(((x^2-1)^i), x, i);
    b(i)=(1/((2^i)*factorial(i)))*d;
end
disp(b);
%% Генератор последовательности Лежандра
% ls - вектор-строка последовательности Лежандра длины p,
где p-нечетное простое число.
% Последовательность Legendre может использоваться для
формирования двоичных последовательностей с хорошим
% корреляционными свойствами.
clear;
close all;
p = 13; %p-нечетное простое число
```

```
ls = qrseq(p); %Квадратичные последовательности остатков
- QRSEQ.
disp(ls);
function ls = qrseq(p)
if p<3 || ~isprime(p) %значение isprime истинно, когда p
является простым числом. В противном случае-значение
false
error('qrseq:primality', 'p must be an odd prime.'); %p
должно быть нечетным простым числом
end
if eps((p/2)^2) > 1 %eps возвращает положительное
расстояние от abs (x) до следующего большего числа с
плавающей
    %запятой с той же точностью, что и x
error('qrseq:toobig', 'p is too large.');
end
ls = [0 -ones(1,p-1)]; % ones матрица из 1 размера 1 на
p-1
ls(1+mod((1:(p-1)/2).^2,p)) = 1;
end
%% Создаем последовательность в зависимости от
длительности импульса
tau_imp=1; %Длительность импульса
f_disk=20; %Частота дикретизации
dt=1/f_disk; % Дискреты времени - отсчеты по времени
n=length(ls); % Число импульсов
t=0:dt:(n*tau_imp-dt); % Задаем временные отсчеты -задали
временной вектор
kol=n*(tau_imp/dt); % Количестов отсчетов для
полседовательности
```

```
posl(1:kol)=0; %Задаем нулевую последовательность
z=0; %Счетчик
for j=1:length(ls) %Перебор импульсов
for i=1:(f_disk) %Перебор отсчетов для 1 импульса
k=i+f_disk*z; %Задаем номер отсчета, с которого
начинается новый импульс
posl(k)=ls(z+1);
end
z=z+1; %Переход к следующему импульсу
end
%% АКФ [9-10]
n=1:length(posl); %создаем вектор-строку
for i=1:length(posl) %заполняем вектор-строку нулями
n(i)=0;
end
%S_mp1=ls'; %превращаем в вектор-столбец
S_mp1=posl;
n1=[n S_mp1 n]; %складываем массив нулей-сигнал-нулей
n2=[S_mp1 n n];
u=1:(3*length(posl)); % массив для перемножения
for i=1:3*length(posl) %перебор строки
x=n1.*n2; %перемножение сигналов поэлементно
u(i)=abs(sum(x)); %сумма
n2=circshift(n2,1,2);
end
ta=[];b=0;
for i=1:length(u)
ta=[ta b];
b=b+dt;
end
```

```
figure(1);
plot(ta,u,'Color', 'r','LineWidth' ,1);
title ('АКФ')
xlim([0 (2*length(ls)*tau_imp+1)])
figure(3)

%% ВКФ [11]
n=length(ls);
for i=1:n
if mod(i,2)==0
n2_VKF(i)=-1;
else n2_VKF(i)=1;
end
end
% Генерируем последовательность
posl_VKF(1:kol)=0; %Задаем нулевую последовательность
z=0; %Счетчик
for j=1:n %Перебор импульсов
for i=1:(f_disk) %Перебор отсчетов для 1 импульса
k=i+f_disk*z; %Задаем номер отсчета, с которого
начинается новый импульс
posl_VKF(k)=n2_VKF(z+1);
end
z=z+1; %Переход к следующему импульсу
end
%VKF
n=1:length(posl_VKF); %создаем вектор-строку
for i=1:length(posl_VKF) %заполняем вектор-строку нулями
n(i)=0;
end
```

```
%S_mp1=ls'; %превращаем в вектор-столбец
S_mp1=posl_VKF;
n1=[n S_mp1 n]; %складываем массив нулей-сигнал-нулей
n2_VKF=[S_mp1 n n];
u=1:(3*length(posl_VKF)); % массив для перемножения
for i=1:3*length(posl_VKF) %перебор строки
x=n1.*n2_VKF; %перемножение сигналов поэлементно
u_VKF(i)=abs(sum(x)); %сумма
n2_VKF=circshift(n2_VKF,1,2);
end
ta=[];b=0;
for i=1:length(u_VKF)
ta=[ta b];
b=b+dt;
end
figure(2);
plot(ta,u_VKF,'Color', 'r','LineWidth' ,1);
title ('ВКФ')
xlim([0 (2*length(ls)*tau_imp+1)])
```

Результаты

>> generator

$$[x,(3*x^2)/2-1/2,(5*x^3)/2-(3*x)/2]$$

$$[x,3*x^2)/2-1/2,(3*x*(x^2-1))/2+x^3]$$

Формирование полиномов Лежандра

>> generator3

0 1 -1 1 1 -1 -1 -1 -1 1 1 -1 1

Формирование последовательности Лежандра

Входные данные 1: `tau_imp=1; f_disk=20; p = 7;` %длина полинома //рис. 4, 6

Входные данные 2: `tau_imp=2; f_disk=20; p = 7;` %длина полинома//рис. 5, 7

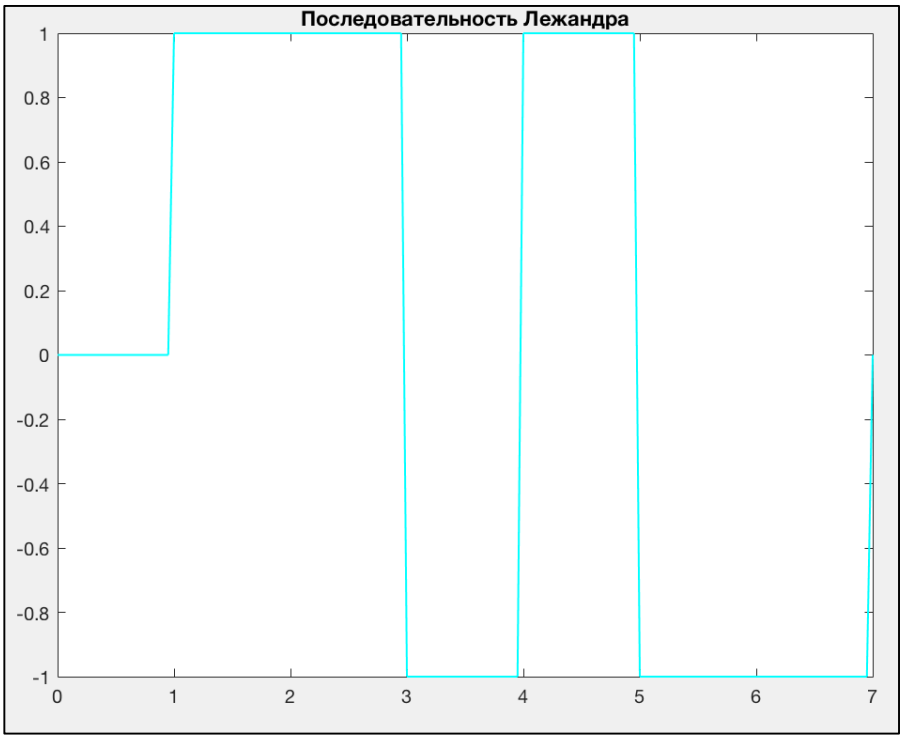

Рис. 2. Последовательность Лежандра

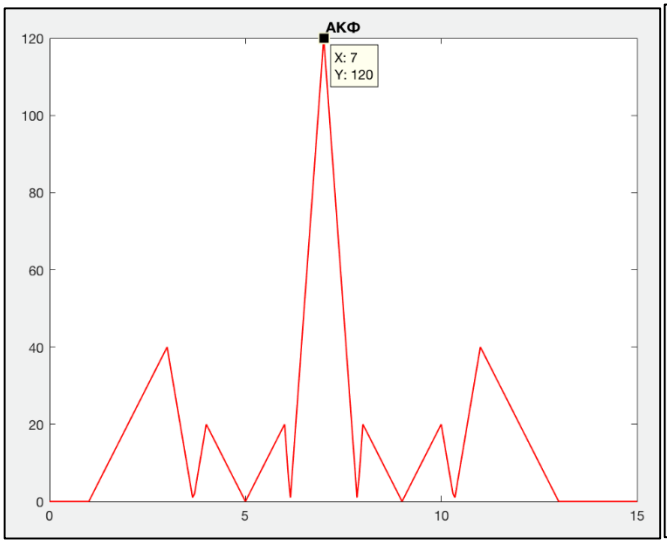

Рис. 3. АКФ

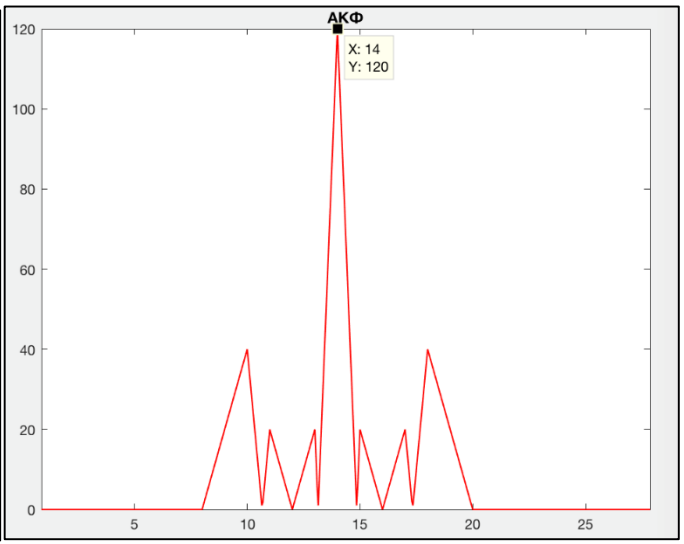

Рис. 4. АКФ

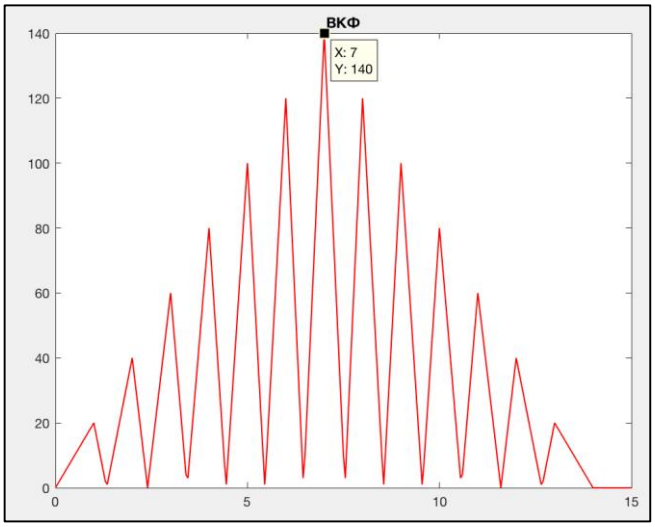

Рис. 5. ВКФ

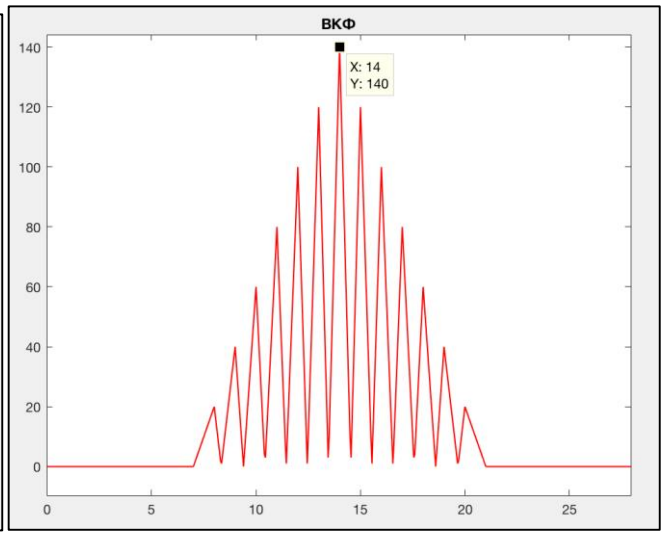

Рис. 6. ВКФ

Анализ скрытности

Арсенальной будем называть **скрытность**, определяемую мощностью A (числом элементов) множества X возможных сменных параметров сигнала, например, несущих частот, вариантов кодовой структуры. Рабочие параметры передаваемого сигнала выбираются из этого множества случайно для противника.

Широкополосными называют сигналы, для которых: $B = FT \gg 1$.

Введем понятие базы передатчика: $\bar{B} = \bar{F}\bar{T}$, где $\bar{T}$ - максимальная длительность сигналов из множества X, а $\bar{F}$ - диапазон частот, в котором могут находиться рабочие сигналы.

Наш сигнал – импульсная последовательность из $M >> 1$ элементов с

длительностью элементарного символа (микроимпульса) τ и общей длительностью сигнала $T = M\tau$. Ширина спектра такого ШПС определяется длительностью микроимпульса τ:

$$F = \frac{1}{\tau} >> \frac{1}{T}$$

Так как ширина спектра сигнала $F = \overline{F} = 1/\tau$, а длительности всех сигналов одинаковы ($T = \overline{T}$) то получим : $A = M = FT = B$

Таким образом, арсенал последовательности (арсенальная скрытность) равен:

$$S = -log_2\left(\frac{1}{A}\right) = log_2(A) = log_2 M = log_2 FT$$

$$S = log_2 FT = log_2 \frac{1}{\tau} * M\tau = log_2 M = log_2 7 = 2{,}8$$

Рассчитаем скрытность еще для нескольких значений М (таблица 1).

Таблица 1 – Расчет скрытностей для нескольких значений М

M	S
7	2,8
11	3,45
13	3,7
17	4,08

Вывод: с увеличением длины полинома Лежандра (М) арсенальная скрытность увеличивается. Структура кодовых последовательностей выбирается таким образом, чтобы при заданном их числе (арсенале) A обеспечить их максимальное взаимное различие, мерой которого являются взаимокорреляционные функции (ВКФ). На приемной стороне широкополосного канала связи принятый ШПС в смеси с помехами сравнивается со всеми копиями передаваемых сигналов с помощью вычисления значений ВКФ, по максимуму которых выбирается переданный информационный сигнал.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Андреева Т.Г. Математика: специальные функции и некоторые приложения. Учебное пособие // Спб.: РГГМУ, 2013. – 38-45.
2. Холодова С.Е., Перегудин С.И. Специальные функции в задачах математической физики. Учебное пособие // Спб.: ИТМО, 2012. – С. 18-26.
3. Свириденко А.А. Свойства ограниченно-плоских аппроксимаций с корректирующими полиномами Лежандра // Минск БГУИР: Информационные технологии и системы 2015 (ИТС 2015), 2015. – С. 316-317.
4. Бирюк А.А. Исследование возможности создания радиофотонной ФАР // Москва: Московский институт электронной техники, 2017 – С. 72-75.
5. Калмыков В.В., Юдачев С.С. Ансамбли составных кодовых последовательностей // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 1994. №4. С. 101-106.
6. Popravko E. D., Maruschenko S. G. // Program realization of search of code sequences with the set correlation properties.
7. Berthold K. P. Horn, Interesting eigenvectors of the Fourier transform, Transactions of the Royal Society of South Africa, Vol. 65(2), June 2010, 100-106
8. P. Borwein, K. K. S. Choi, and J. Jedwab. Binary sequences with merit factor greater than 6.34, IEEE Trans. Inf. Theory, 50(12), December 2004.
9. Солонина А.И., Клионский Д.М., Меркучева Т.В., Перов С.Н. Цифровая обработка сигналов и MATLAB: учеб. пособие // Спб.: БХВ-Петербург, 2013. – С. 337-339.
10. Романов Б.Н., Краснов С.В. Теория электрической связи. Сообщния, сигналы, помехи, их математические модели. Учебное пособие // Ульяновск: Ульяновский государственный технический университет, 2008. – С. 45-51.
11. Баскаков С.И. Радиотехнические цепи и сигналы // М.: Высшая школа, 1988. – С. 68-83.