ВЗАИМНАЯ КОРРЕЛЯЦИЯ М И GMW ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Кренгель Е.И., А. З. Тиркел и Т.Е. Холл

KEDAH ELECTRONICS ENGINEERING, Россия, Москва,
Тел. (095) 530-46-16б,E-mail: kedah@mail.compnet.ru;
Отделение математики и статистики Монашского Университета, Австралия,
Тел./Факс +61-3-95922206

Реферат. В докладе анализируются пиковые значения взаимной корреляции m и GMW последовательностей. Такие последовательности выражаются в виде матриц, где каждый столбец за исключением столбцов из нулей является циклическим сдвигом короткой псевдослучайной последовательности. Сверхвысокая корреляция является результатом совпадения большого числа столбцов. Теоретически точно предсказываются пары последовательностей и их циклические сдвиги, дающие сверхвысокую корреляцию. Учет этих сдвигов позволяет создавать большие подмножества последовательностей с хорошей взаимной корреляцией. Это может быть использовано для систем связи с CDMA и цифровых водяных знаков изображений.

Введение

Периодическая взаимная корреляция двоичных m и GMW последовательностей проанализирована теоретически, а также статистическими и вычислительными методами. Исчерпывающий компьютерный поиск всех взаимных корреляций m-последовательностей в настоящее время ограничен диной 2^{25}-1. Статистический анализ взаимной корреляции m-последовательностей с помощью методов Фурье был предпринят еще в 1965г. [1]. При этом были обнаружены некоторые неожиданно большие значения взаимной корреляции, достигающие 1/3 автокорреляционного пика и не уменьшающиеся с увеличением длины последовательности. Эти “аномальные” значения были исследованы в [2], где они были отнесены к конечным арифметическим эффектам. В [3] было показано, что некоторые пары GMW последовательностей имеют точно такие же значения взаимной корреляции, что и m-последовательности. Эти исследования показали, что пары последовательностей с высокой взаимной корреляцией предсказуемы, но в предсказанных их пиковых значениях имеются ошибки.

Настоящая работа представляет теорию, которая **точно** предсказывает высокую взаимную корреляцию для m и всех GMW последовательностей. Это достигается размещением последовательностей вдоль диагоналей двумерных матриц [4]. Мы исследуем матрицы, в которых столбцы являются либо сдвигами короткой последовательности, либо последовательностью из нулей. Такие форматы существуют для всех m-последовательностей длины 2^n-1, где n составное число. Последовательность циклических сдвигов порождается исходной m-последовательностью и ее образующим полиномом [5]. Можно доказать, что если короткую m-последовательность в такой матрице заменить другой идеальной псевдослучайной последовательностью с теми же сдвигами, то в результате получится последовательность GMW [6]. Ниже рассматривается декомпозиция m-последовательности длины 2^{2m}-1 в "квадратную" матрицу из 2^m+1 столбцов длины 2^m-1 для всех нечетных m≥3. Все m-последовательности могут быть образованы с помощью надлежащей децимации из любой m-последовательности. Такие децимации могут быть сведены к децимациям столбцов с перестановкой порядка их следования в матрице декомпозиции.

Теорема

Пусть $n=2m$, где $m\geq 3$ нечетно. Пусть $\{\alpha i\}$ и $\{b_i\}$ есть m или GMW последовательности, где $\{b_i\}$ связана децимацией $d_r=r(2^n-1)/3+1$ с $\{\alpha i\}$, где $r=1$ or 2 порождает надлежащую децимацию. Тогда максимальная взаимная корреляция этих последовательностей принимает следующие значения:

если m не кратно 3: $(2^{2m}-2^{m+1}-3)/3$ (дважды); $(2^{2m}+2^{m+2}-3)/3$ (один раз)

если m кратно 3 : $(2^{2m}-2^{m+1}-3)/3$ (один раз); $(2^{2m}+2^m-3)/3$ (дважды).

Идея доказательства

Данные матрицы состоят из 2^m столбцов, являющимися циклическими сдвигами m-последовательности и одного столбца из нулей. Последовательность сдвигов состоит из 2^{m-1} чисел, каждое из которых повторяется дважды и указателя нулей (символ "-"), т.е. всего из 2^m+1 элементов. При этом последовательность сдвигов представляет собой палиндром с осью симметрии относительно нулевого столбца [7]. Децимация d при представлении последовательности вдоль диагоналей матрицы соответствует децимации столбцов $d_C=d$ *(Modulo* 2^m*-1)* и децимации рядов $d_R=d$ *(Modulo* 2^m*+1).* Децимации, ведущие к большому выбросу [2], имеют вид $\frac{r(2^{2m}-1)}{q}+1$, где q делитель 2^{2m}-1 и r есть целое, меньшее q. Для этих децимаций $d_C=1$, где $\frac{r(2^m+1)}{q}$ есть целое, т.е. q также является делителем 2^m+1. Это означает, что обе матрицы имеют одни и те же столбцы, но в различном порядке. Значение $d_R=\frac{r(2^m+1)}{q}+1$ определяет порядок перестановки столбцов. В этом случае взаимная корреляция определяется числом совпадающих столбцов. Каждое совпадение вносит 2^m-1, тогда как каждое несовпадение вносит -1. *Столбцы* могут совпадать в двух случаях, если (i) столбец при децимации остается на месте или (ii) переходит в свое отражение. Пусть $q=3$, а k есть относительный горизонтальный сдвиг матриц.

(i) Уравнение $\boldsymbol{d_R i}=\boldsymbol{i}+\boldsymbol{k}$ имеет $\frac{(2^m+1)}{3}$ решений при $k=0$, $k=\frac{(2^m+1)}{3}$ и $\frac{2(2^m+1)}{3}$.

(ii) Уравнение $\boldsymbol{d_R i}=-\boldsymbol{i}+\boldsymbol{k}$ имеет единственное решение, когда $(\boldsymbol{d_R}+1)$ имеет обратный по умножению элемент по modulo 2^m+1. Если n кратно *3*, то для всех $k\neq 0$ имеется еще одно дополнительное совпадение. Если n не кратно *3*, то имеются два дополнительных совпадения при $k=0$ и ни одного при других k .остальных.

Результаты, вытекающие из теоремы

Для *n=6* максимум взаимной корреляции есть *+23* (дважды) и один раз *+15*
Для *n=10* максимум взаимной корреляции есть *+383*(раз) и дважды +319.
Для *n=14* максимум взаимной корреляции есть *+5631*(раз) и дважды *+5375.*
Для *n=18* максимум взаимной корреляции есть *+87551* (дважды) и один раз *+87039.*
Для *n=22* максимум взаимной корреляции есть *+1400831*(раз) и дважды *+1396735.*

Эти результаты совпадают с результатами непосредственных расчетов, проведенных на компьютере.

Пример

Эффективность теории проиллюстрируем на небольшом примере для *n=6*. В соответствие с нашей теорией предсказанные децимации есть *63/3+1=22* and *2×63/3+1=43*. Рассмотрим случай *d=22.* Всего имеется 9 столбцов длины 7 с $d_C=1$ and $d_R=4$. Столбцы отображаются сами в себя, когда $\boldsymbol{d_R i}=\boldsymbol{i}+\boldsymbol{l}\frac{2^n+1}{3}$ или в нашем случае $4\boldsymbol{i}=\boldsymbol{i}+3\boldsymbol{l}$.

Столбцы переходят в свои отражения, когда $\boldsymbol{d_R i}=-\boldsymbol{i}+\boldsymbol{l}\frac{2^n+1}{3}$ или $4\boldsymbol{i}=-\boldsymbol{i}+3\boldsymbol{l}$. Для *l=0* второе уравнение не имеет решений, тогда как первое имеет 3 решения. В результате 3 столбцы с номерами *0,3,6* совпадают. Для *l=1* решения первого уравнения есть *1,4,7*, а второе уравнение сводится к $5\boldsymbol{i}=3$. Поскольку *2* имеет обратное по умножению число *5* по модулю *9*, то последнее уравнение имеет единственное решение $\boldsymbol{i}=5^{-1}\times 3=2\times 3=6$.

В итоге имеем 4 совпадающих столбцов с номерами *1,4,6,7* .

Для наглядности ниже изображены матрицы декомпозиции рассматриваемых m-последовательностей. Слева представлена матрица декомпозиции исходной m-последовательности длины *63*. Над ней расположена последовательность сдвигов. Справа изображена матрица, соответствующая децимации 22, со своей последовательностью сдвигов.

Исходная Матрица

Последовательность сдвигов

-	4	3	5	1	1	5	3	4

0 0 0 1 0 0 1 0 0
0 0 1 0 1 1 0 1 0
0 1 0 0 1 1 0 0 1
0 0 1 1 1 1 1 1 0
0 1 1 0 0 0 0 1 1
0 1 1 1 0 0 1 1 1
0 1 0 1 1 1 1 0 1

<u>Децимация *d=22*</u>

Последовательность сдвигов

-	3	1	5	4	4	5	1	3

0 0 0 1 0 0 1 0 0
0 1 1 0 0 0 0 1 1
0 0 1 0 1 1 0 1 0
0 1 1 1 0 0 1 1 1
0 1 0 0 1 1 0 0 1
0 1 0 1 1 1 1 0 1
0 0 1 1 1 1 1 1 0

При нулевом сдвиге совпадают нулевые столбцы, а также столбцы со сдвигом 5. В этом случае взаимная корреляция равна *3×7-6=+15*. Рассмотрим матрицу децимации 22 с горизонтальным сдвигом на 3. Последовательности сдвига для этого случая показаны ниже.

-	4	3	5	1	1	5	3	4
5	4	4	5	1	3	-	3	1

Столбцы с номерами *1,4,6,7* совпадают, порождая взаимную корреляцию *4×7-5=+23*.

Заключение

Полученная теория может быть использована при выборе последовательностей в системах CDMA. Для асинхронных CDMA все указанные децимации могут быть удалены. Например, в случае *n=14* классы эквивалентности m-последовательностей и последовательностей GMW содержат по *756* последовательностей. После удаления *d=5462* остается *378* последовательностей. В результате этого для m-последовательностей максимальная взаимная корреляция уменьшается с *+5631* до *+897*, т.е. на *16dB*. Очевидно, что для случая квазисинхронных CDMA существует возможность избежать найденных “вредных” фазовых сдвигов. Следовательно, могут быть использованы все *756* последовательностей из любого класса.

Библиография

[1] R.Gold, E.Kopitzke, “Study of correlation properties of binary sequences” Interim Tech Report 1, vol 1-4, Magnavox Res Labs, Torrance, CA, (AD470696-9) 1965.

[2] A.Z. Tirkel, C.F. Osborne, T.E. Hall, “Effects of bias and characteristic phase on cross-correlation of m-sequences”, IEE Proc.- E, **144**, (4), 217-220, August 1997.

[3] Кренгель Е.И., Мешковский К.А. Взаимная корреляция некоторых классов псевдослучайных последовательностей. – Радиотехника, N6, стр. 8-13, 2000.

[4] F.J. Macwilliams, N.J.A. Sloane, “Pseudo-Random Sequences and Arrays”, Proceedings of the IEEE, Dec.1976, **64** (12), 1715-1729.

[5] L. Weng “Decomposition of m-sequences and its applications” IEEE IT-**17**, 457-463, 1971.

[6] Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча. - Техника средств связи, Сер. ТРС, вып. 3, стр. 17-30, 1979.

[7] D.H. Green, ‘Structural Properties of Pseudorandom Arrays and Volumes and Their Related Sequences,’ IEE Proceedings - E, May 1985, 132 (3) pp. 133-145

CROSS-CORRELATION OF M AND GMW SEQUENCES

E.M. Krengel, A.Z.Tirkel€ and T.E.Hall€

KEDAH ELECTRONICS ENGINEERING, Moscow, Russia,
Ph (095) 530-4616, E-mail: kedah@mail.compnet.ru
€Department of Mathematics and Statistics, Monash University, PO Box 28M, Victoria 3800, Australia.
Ph/Fax +61-3-95922206

Abstract. This paper analyses peaks in the cross-correlation between m-sequences and GMW sequences. Such sequences are expressed as matrices, where each column (apart from a single null column) is a cyclic shift of a pseudonoise sequence. The highest cross-correlations are due to many columns being forced to match. The theory is precise and is able to predict the pairs of sequences and cyclic shifts giving the largest cross-correlation. Avoidance of offending sequences or cyclic shifts allows the production of large sets of pseudonoise sequences with good cross-correlation. This is useful for CDMA and digital watermarking of images.

Introduction

The periodic cross-correlation of binary m-sequences and of GMW sequences has been analysed theoretically and by statistical and computational means. Exhaustive computer search of all cross-correlations is at present limited to m-sequences of length below about $2^{25}-1$. Statistical analysis of m-sequence cross-correlations by Fourier techniques was attempted as far back as 1965 [1]. This revealed some unexpectedly high cross-correlation values for m-sequences of compound length. *These values are as high as 1/3 of the autocorrelation peak and do not diminish with increasing sequence length*. These "anomalous" values were analysed in [2], where they were attributed to finite arithmetic effects. In [3] it was shown that some pairs of GMW sequences have exactly the same high cross-correlation values. That analysis showed that the pairs of sequences with high cross-correlation were predictable, but there were residual errors in the predicted values.

This paper presents a theory, which predicts high cross-correlations of m-sequences precisely and extends the above framework to all GMW sequences. It is achieved by placing the sequences along the diagonals of two-dimensional arrays [4]. We make use of representations where the columns are shifts of a shorter m-sequence or are null (constant) columns. Such formats are available for all m-sequences whose lengths are 2^n-1, with n composite. The sequence of cyclic shifts (shift sequence) is peculiar to the parent m-sequence [5]. It can be proved that if the shorter m-sequences in such an array are replaced by other ideal pseudonoise sequences with the same shifts, we will get GMW sequences [6]. The cross-correlation of two arrays can be expressed as the sum of the cross-correlations of the columns. Here, we consider the decomposition of an m-sequence of length $2^{2m}-1$ into a “square” array of 2^m+1 columns of length 2^m-1, with odd $m\geq 3$. All m-sequences of a particular length are generated by proper decimations of any m-sequence. Such decimations can be translated into decimations of column sequences and permutations of the order of columns in the arrays.

Theorem

Let $n=2m$, with $m\geq 3$ odd. Let $\{a_i\}$ and $\{b_i\}$ be m-sequences or GMW sequences, with $\{b_i\}$ being the decimation $d_r=r(2^n-1)/3+1$, of $\{a_i\}$, where $r=1$or 2, whichever yields a proper decimation. Then, the worst case cross-correlation of these sequences has the following values:

a) for m not divisible by 3: $(2^{2m}-2^{m+1}-3)/3$ (twice); $(2^{2m}+2^{m+2}-3)/3$ (once)

b) for m divisible by 3 : $(2^{2m}-2^{m+1}-3)/3$ (once); $(2^{2m}+2^{m}-1)/3$ (twice).

Example

A small example, $n=6$, is shown below as an illustration of the theory.

Our theory predicts the offending decimations to be $63/3+1=22$ and $2\times 63/3+1=43$

Consider $d=22$. Since the column length is 7 and there are 9 columns, $d_C=1$ and $d_R=4$.

Columns will be permuted to fall upon themselves when $d_R i = i + l\dfrac{2^m+1}{3}$ or $4\boldsymbol{i} = \boldsymbol{i} + 3\boldsymbol{l}$ for this case. Columns will be permuted to overlay their images when

$d_R i = -i + l\frac{2^m+1}{3}$ or $4\boldsymbol{i} = -\boldsymbol{i} + 3\boldsymbol{l}$. For *l=0*, there are no solutions to the latter equation, whilst there are *3* to the previous equation. Therefore, *3* columns, those indexed *0,3,6,* match. For *l=1,* the solutions to the previous equation are *1,4,7* and the latter equation implies $5\boldsymbol{i} = 3$. Now, *2* is a multiplicative inverse of *5 (modulo 9)* and so the latter equation has a unique solution $\boldsymbol{i} = 5^{-1} \times 3 = 2 \times 3 = 6$.

Finally, we have obtained the result that the columns labeled *1,4,6,7* match.

The observed situation is shown below. A prototype m-sequence of length *63* is decomposed into an array of *9* columns each of length *7*, shown on the left. The shift sequence is shown above. A decimation leading to high bias is: *63/3+1=22*. The array decimated by *22* is shown to the right, with its shift sequence above it.

Prototype Array

Shift Sequence

-	4	3	5	1	1	5	3	4

0 0 0 1 0 0 1 0 0
0 0 1 0 1 1 0 1 0
0 1 0 0 1 1 0 0 1
0 0 1 1 1 1 1 1 0
0 1 1 0 0 0 0 1 1
0 1 1 1 0 0 1 1 1
0 1 0 1 1 1 1 0 1

Decimation *d=22*

Shift Sequence

-	3	1	5	4	4	5	1	3

0 0 0 1 0 0 1 0 0
0 1 1 0 0 0 0 1 1
0 0 1 0 1 1 0 1 0
0 1 1 1 0 0 1 1 1
0 1 0 0 1 1 0 0 1
0 1 0 1 1 1 1 0 1
0 0 1 1 1 1 1 1 0

For asynchronous CDMA, the offending decimation can be removed. For *n=14* there is a total of *756* m-sequences. Removing *d=5462* leaves *378* sequences in the set. This reduces the peak cross-correlation from *+5631* to *+897*, a reduction of *16dB*. For quasi-synchronous CDMA it is possible to avoid the offending phase shifts, in which case the full set of *756* sequences could be used.

References

[1] R.Gold, E.Kopitzke, "Study of correlation properties of binary sequences" Interim Tech Report 1, vol 1-4, Magnavox Res Labs, Torrance, CA, (AD470696-9) 1965.

[2] A.Z. Tirkel, C.F. Osborne, T.E. Hall, "Effects of bias and characteristic phase on cross-correlation of m-sequences", IEE Proc.- E, **144**, (4), 217-220, August 1997.

[3] E.I.Krengel, K.A.Meshkovskii, "Cross-correlation of some classes of pseudo-noise sequences", Radio Engineering and Technology, 8-13, June 2000.

[4] F.J. Macwilliams, N.J.A. Sloane, "Pseudo-Random Sequences and Arrays", Proceedings of the IEEE, Dec.1976, **64** (12), 1715-1729.

[5] L. Weng "Decomposition of m-sequences and its applications" IEEE IT-**17**, 457-463, 1971.

[6] E.I. Krengel. "About the number of Gordon, Mills, Welch pseudo random sequences", Engineering of the communication facility, series of Radio engineering, Issue 3, Moscow, 1979.