Do the Barker Codes End?
A Problem for the WPI MPI Workshop

Greg Coxson
Technology Service Corporation
Silver Spring, Maryland

WPI, Worcester, MA
16 to 20 June, 2008

Some Motivation from the World of Radar

An Early Radar Tradeoff

Two performance objectives:

- Long detection ranges.
- Good range resolution.

How to get both at the same time?

Detection Range

Consider a simple radar signal:

- Rectangular pulse of width T.
- Constant transmit power P.

Long detection ranges depend on getting as much energy on the target as possible.

The only option: make T as large as possible.

Range Resolution

Resolution is the minimum distance between two targets for which a radar sees them as two separate targets.

Range resolution is proportional to the pulse width T.

Range resolution is improved by making T small.

Achieving Resolution and Detection Range

- Long detection range means longer pulses.
- Good resolution requires short pulses.

What if we want both at the same time?

Answer: Pulse compression.

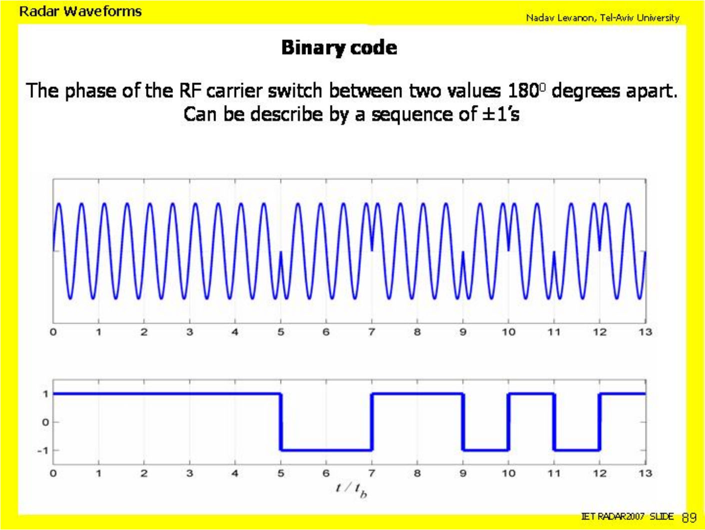
Basics of Pulse Compression and Barker Codes

Pulse Compression

Pulse compression works as follows:

- Divide a radar pulse into N equal-width subpulses.
- Before transmitting, apply a phase shift to each subpulse, either:
  - Zero degrees (that is, multiply subpulse by 1).
  - 180 degrees (i.e., multiply subpulse by -1).
- Save the sequence of 1 and -1 factors as N-length "code" x.
- When the radar pulse return is received, apply a Matched Filter using the same code x.

Illustration of Pulse Encoding



The Binary Code Space

A binary code x is a sequence of elements

$$x = [x_1, x_2, \ldots, x_N]$$

where

$$x_i \in \{-1, 1\}$$

for $i = 1, \ldots, N$, where N is its length.

Then the code *alphabet* is

$$S_2 = \{-1, 1\}$$

and the *code space* is

$$S_2^N = S_2 \times S_2 \times \ldots \times S_2$$

(the Cartesian product of N copies of S_2).

Matched Filter Response

For $x \in S_2^N$, The response of the matched filter is the autocorrelation of x:

$$\mathrm{ACF_x = x * \overline{x}}$$

where $\overline{x}$ is the reversal of x and $*$ represents aperiodic convolution.

The autocorrelation is a sequence of length $2N - 1$. Element k can be written in terms of code elements x_i as:

$$\mathrm{ACF_x(k)} = \sum_{\mathrm{i=1}}^{\mathrm{N-|k|}} \mathrm{x_i x_{i+|k|}}.$$

for any k, $-(N-1) \leq k \leq N - 1$.

Example

$$
\begin{aligned}
x &= [x_1, x_2, x_3, x_4] \\
&= [1, 1, -1, 1]
\end{aligned}
$$

Then

$$
\begin{aligned}
\mathrm{ACF_x}(1) &= x_1 * x_2 + x_2 * x_3 + x_3 * x_4 = 1 - 1 - 1 = -1 \\
\mathrm{ACF_x}(2) &= x_1 * x_3 + x_2 * x_4 = -1 + 1 = 0 \\
\mathrm{ACF_x}(3) &= x_1 * x_4 = 1
\end{aligned}
$$

Properties of the Autocorrelation

- For $x \in S_2^N$, $\mathrm{ACF_x}$ has length $2N - 1$.
- $\mathrm{ACF_x(0) = N}$ (the "peak").
- $\mathrm{ACF_x(k)}$ for $1 - N \leq k \leq N - 1$, $k \neq 0$, is a "sidelobe".
- $\mathrm{ACF_x(k) = ACF_x(2N - k)}$ for $k = 1 - N, \ldots, N - 1$ (the autocorrelation is symmetric).
- The peak sidelobe level $(\mathrm{PSL_x})$ is the maximum sidelobe size:

$$\mathrm{PSL_x} = \max_{\mathrm{k \neq 0}} |\mathrm{ACF_x(k)}|.$$

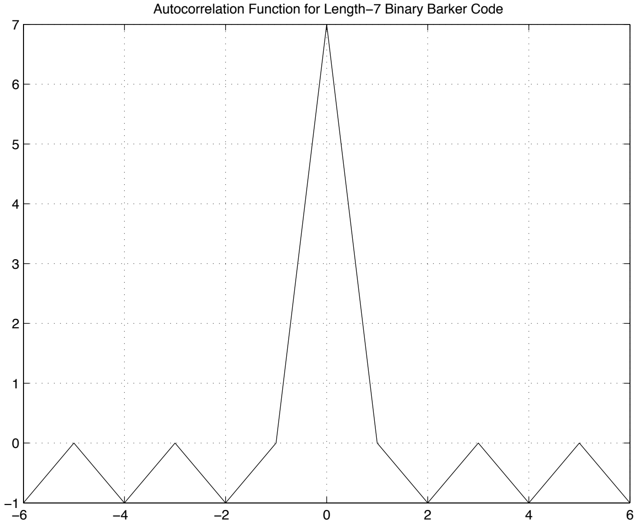
The Importance of Low Peak Sidelobe Level

Suppose there are undesired point targets in the vicinity of a target of interest.

Then:

- Ideally the desired target will experience the peak response.
- The response for the undesired targets should be as low as possible to avoid declaring false detections.

Autocorrelation of a Length-7 Barker Code



The Binary Barker Codes

For any binary code x:

- $\mathrm{PSL_x}$ is a positive integer.
- $\mathrm{PSL_x} \geq 1$.

A binary code x for which $\mathrm{PSL_x} = 1$ is a *Barker Code*.

Operations Preserving Peak Sidelobe Level

There are three operations that preserve peak sidelobe level in binary codes:

- Reversal: $Rx = \overline{x}$.
- Negation: $Nx = -x$.
- Alternating sign: $Px = xA$ where

$$A = \mathrm{Diag}(1, -1, 1, \ldots, (-1)^{\mathrm{N}-1}).$$

The PSL-Preserving Operator Groups

The PSL-preserving operations generate two groups, one for odd code lengths and one for even code lengths.

For odd code lengths, R, N and P generate an Abelian group isomorphic to $Z_2 \times Z_2 \times Z_2$.

For even code lengths, R, N and P generate a non-Abelian dihedral-8 group.

Equivalence Classes

For $y, x \in S_2^N$ define the relation $y \sim x$ to mean that y can be formed from x by some combination of the three PSL preservers.

$y \sim x$ is easily seen to be an equivalence relation.

S_2^N is partitioned into equivalence classes of size either 8 or 4.

The equivalence class of any odd-length binary Barker code has size 4 (The peak sidelobe preserver group action on the odd-Barkers degenerates due to a shared symmetry known of as Golay's skew-symmetry).

The Known Binary Barkers

All known binary Barkers are equivalent to the following codes:

- $N = 2$: $[1, 1]$ and $[1, -1]$.
- $N = 3$: $[1, 1, -1]$.
- $N = 4$: $[1, 1, 1, -1]$ and $[1, 1, -1, 1]$.
- $N = 5$: $[1, 1, 1, -1, 1]$.
- $N = 7$: $[1, 1, 1, -1, -1, 1, -1]$.
- $N = 11$: $[1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1]$.
- $N = 13$: $[1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1]$.

The Main Problem

There are no Barker codes of odd length greater than 13 (Turyn and Storer, "On binary sequences", *Proceedings of the AMS*, volume 12 (1961), pages 394-399.):

The existence of even-length Barkers for $N > 4$ remains open.

Problem 1. Is there a largest $N < \infty$ for which a binary Barker Code of length N exists?

A Good Resource

An excellent summary of developments on solving Problem 1:

Jedwab, J., "What can be used instead of a Barker sequence?", submitted to *Contemporary Mathematics*.

Key Results for Binary Barker Codes

Theorem. if there exists a binary Barker code of even length $N > 4$, then $N = 4S^2$ for some odd integer $S \geq 55$ that is not a prime power. (Turyn, R., "Character sums and difference sets", Pacific Journal of Mathematics, volume 15 (1965), pages 319-346.

Theorem. If there exists a Barker sequence of even length N then N has no prime factor congruent to $3 \bmod 4$. (Eliahou, S., Kervaire, M. and Saffari, B., "A new restriction on the lengths of Golay complementary sequences", *Journal of Combinatorial Theory (A)*, volume 55 (1990), pages 49-59).

Theorem. There is no Barker sequence of length N for $13 < N < 10^{22}$. (Leung, K., and Schmidt, B., "The field descent method", *Design, Codes and Cryptography*, volume 36, pages 171-188).

An Approach

To get a handle on the proportion of Barker codes in S_2^N for a given N, one approach that has been tried:

- Assume the code elements are random variables.
- Assume the pairwise products in sidelobe sums are statistically independent.
- View the sidelobe sums as random walks.
- Assume the sidelobes are statistically independent.
- Find the probability of a Barker Code of length N as the product of probabilities that all the random walks return to the interval $[-1, 1]$ in the appropriate number of steps.

The Devil in the details: at lower PSL values, the sidelobe independence assumption breaks down.

The idea might be made to work if a good model of dependence can be found and exploited.

Barkers Beyond Binary

Generalized Barker Sequences

Consider generalizing the code alphabet from S_2 to

$$S_m = \{\exp(i2\pi k/m) : k = 0 : m-1\}.$$

for $m \geq 2$.

In other words, S_m is the set of the m^{th} roots of unity.

Then

$$S_m^N = S_m \times S_m \times \ldots \times S_m$$

the Cartesian product of N copies of S_m.

Terminology

Codes $x \in S_m^N$ for $m > 2$ are referred to using several names, and the usage is not standardized:

- Generalized Sequence – code elements are m^{th} roots of unity. (often, N-Phase sequence means the same thing).
- Polyphase Sequences – unit magnitude is assumed, but no constraint on phase.
- Unimodular Sequences – code elements have unit magnitude.

Autocorrelation Function for Polyphase Sequences

For $x \in S_m^N$, $m \geq 2$, the autocorrelation of x is :

$$\mathrm{ACF_x = x * \overline{x^*}}$$

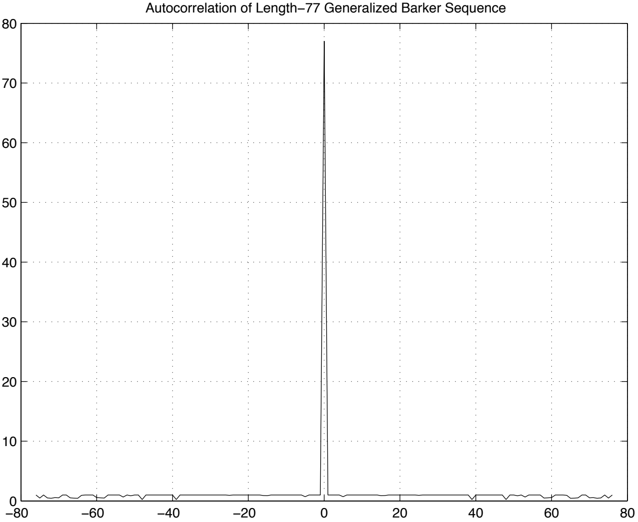
where $\overline{x^*}$ is the conjugate reversal of x.

The autocorrelation so defined remains a sequence of length $2N - 1$. Element k can be written in terms of code elements x_i as:

$$\mathrm{ACF_x(k) = \sum_{i=1}^{N-|k|} x_i x^*_{i+|k|}}.$$

for any k, $-(N-1) \leq k \leq N-1$.

Autocorrelation Function for a Length-77 Barker Sequence



Some Differences With the Binary Case

- Sidelobes may be complex quantities.
- Except for the extreme sidelobes on each side, sidelobes can have any size between 0 and 1.
- $\mathrm{ACF}_{\mathrm{x}}$ is Hermitian.
- There are four operations that preserve PSL.

More Terminology

Define:

The set of N-length $m - phase$ Barker sequences:

$$B_m^N = \{x \in S_m^N : \mathrm{PSL_x} = 1\}$$

The set of N-length *Generalized Barker Sequences*:

$$B^N = \bigcup_{m>2} B_m^N.$$

The set of N-length *Barker Sequences*:

$$B_0^N = \bigcup_{m\geq 2} B_m^N.$$

Generalizing the Problem

Problem 2. Is there a largest $N < \infty$ for which B_0^N is nonempty?

If Problem 2 can be answered in the positive, Problem 1 can be answered in the positive.

PSL-Preservers for Generalized Barkers

The following four operations preserve PSL for polyphase sequences:

- $Cx = x^*$ (Conjugation).
- $Rx = \overline{x}$ (Reversal).
- $M_\mu x = \mu x$, where $|\mu| = 1$ (Multiplication).
- $P_\rho x = x\mathrm{Diag}(\{\rho^0, \rho, \rho^2, \ldots, \rho^{\mathrm{N}-1}\})$ where $|\rho| = 1$ (Progressive Multiplication).

Note:

- When m is specified, and a mapping from S_m^N to S_m^N is needed, then μ and ρ need to be restricted to m^{th} roots of unity.
- When restricting to real codes, the four operations reduce to the three we saw before.

A Question about Group Structure

Question: For a given m, what is the structure of the associated PSL-preserver group?

(My TSC lecture "Theory of groups and low-sidelobe phase coding" (25 June 2007) identifies the structure of groups for odd lengths N. I do not know if the structure for even N is known.)

Equivalence Classes

For $x \in S_m^N$, the equivalence class relative to the four PSL-preservers has size $4m^2$.

The four operations again generate a group. But now:

- There are m groups, depending on $N \mod m$.
- The groups are non-Abelian.

Normalized Sequences

Define an equivalance relation similar to that for the binary codes.

Any generalized sequence x is equivalent to one with its first two elements equal to 1.

The term *Normalization* will refer to the representation of a sequence x by its equivalent with first two elements set to 1.

Number of Normalized Generalized Barkers

Borwein and Ferguson, “Barker Sequences”, CMS-MITACS 2007:

N/m	2	3	4	5	6	7	8	9	10	11	12
6	0	0	0	0	1	0	0	0	0	0	1
7	1	1	1	0	7	0	6	6	12	7	64
8	0	0	0	0	9	1	4	5	10	6	72
9	0	2	0	1	18	4	17	37	72	73	367
10	0	0	0	0	11	0	1	2	7	0	99
11	1	0	1	0	7	0	3	1	12	2	92
12	0	0	0	0	3	0	1	0	0	0	9
13	1	0	1	0	9	0	3	0	14	3	156
14	0	0	0	0	1	0	0	0	1	0	9
15	0	0	1	0	1	0	1	0	4	0	47
16	0	0	0	0	0	0	1	0	0	0	7
17	0	0	0	0	0	0	0	0	0	0	7
18	0	0	0	0	1	0	0	0	0	0	1

Patterns in the Number of Generalized Barkers

Let $Q_N(m)$ represent the number of normalized Generalized Barkers of length N with m phases.

Then

$$Q_N(km) \geq Q_N(m)$$

for $k \geq 1$ an integer.

Note also that the length-6 case is special. If the number of phases is a multiple of 6, there is exactly one normalized Barker. Otherwise, there are none.

The Quaternary Sequences

For radar engineers, $m = 4$ (the quaternary sequences) are almost as useful as the binary codes.

Question: Where do the quaternary sequences end?

Lowest PSL for Quaternary Codes, to Length 24

N	Min PSL	No. Seqs.	N	Min PSL	No. Seqs
2	1	1	14	$\sqrt{2}$	1
3	1	1	15	1	1
4	1	2	16	$\sqrt{2}$	5
5	1	1	17	$\sqrt{2}$	3
6	$\sqrt{2}$	7	18	2	17
7	1	1	19	2	15
8	$\sqrt{2}$	14	20	2	6
9	$\sqrt{2}$	17	21	2	14
10	$\sqrt{2}$	12	22	2	4
11	1	1	23	2	1
12	$\sqrt{2}$	9	24	2	1
13	1	1			

Barkers – Needed Alphabet Size Tends to Grow with N

Borwein and Ferguson, "Barker Sequences", CMS-MITACS 2007:

N	$\min(\lvert \mathrm{ACF_x} \rvert_\infty)$	$\min(m)$	N	$\min(\lvert \mathrm{ACF_x} \rvert_\infty)$	$\min(m)$
37	.818	48	52	.939	95
38	.820	34	53	.918	70
39	.872	48	54	.823	45
40	.871	40	55	.944	90
41	.842	41	56	.965	150
42	.894	50	57	.897	67
43	.842	42	58	.963	295
45	.898	59	59	.976	280
46	.847	42	60	.951	145
47	.888	51	61	.983	400
48	.885	54	62	.931	100
49	.899	54	63	.965	235
50	.916	76	64	.964	206
51	..830	42	65	.983	412

($\lvert \mathrm{ACF_x} \rvert_\infty$ excludes extreme outer sidelobes)

A Conjecture of Ein-Dor *et al*

Ein-Dor, L., Kanter, I. and Kinzel, W., "Low autocorrelated multiphase sequences", *Physical Review E*, volume 65 (2002):

Conjecture: an m-phase generalized Barker sequence of length N exists for all $m \geq N$ and sufficiently large N.

They assume Golay's "Postulate of Mathematical Ergodicity" (essentially, statistical independence of sidelobes).

Question: Is there a point where increasing the alphabet size m fails to deliver the needed marginal benefit as N grows?

Barkers and Littlewood Polynomials

Let $f(z)$ be a Littlewood polynomial of order $N-1$ defined as:

$$f(z) = \sum_{j=0}^{N-1} a_j z^j$$

where $a_j \in \{1, -1\}$ for $j = 0, \ldots, N-1$.

Define the p-norm of $f(z)$ as

$$||f||_p = \left(\int_0^1 |f(\exp(i2\pi t))|^p dt \right)^{1/p}.$$

A popular measure of sidelobe level is Merit Factor, defined as

$$\mathrm{MF(ACF)} = \frac{\mathrm{N}^2}{2\sum_{\mathrm{k}=1}^{\mathrm{N}-1} |\mathrm{ACF(k)}|^2}.$$

Barkers and Littlewood Polynomials, Continued

Borwein and Mossinghoff (ref. 4) show that for sequence $\{\mathrm{ACF(k)}\}$, $1 \leq k \leq N-1$, the Littlewood polynomial formed from the sequence must obey:

$$\mathrm{MF(f)} = \frac{||\mathrm{f}||_2^4}{||\mathrm{f}||_4^4 - ||\mathrm{f}||_2^4}.$$

If the coefficients of polynomial $f(z)$ form a Barker sequence of length N, then

$$||f||_4 \leq \sqrt{N} + \frac{1}{4\sqrt{N}}.$$

To show that long Barker sequences do not exist, it suffices to prove that for all Littlewood polynomials $f(z)$ of a sufficiently large N,

$$||f||_4 > \sqrt{N} + \frac{1}{4\sqrt{N}}.$$

Barker Sequence Spectra

Note that the Fourier transform of the autocorrelation is:

$$\begin{aligned} F(\mathrm{ACF_x}) &= F(x * \overline{x^*}) \\ &= |F(x)|^2 \end{aligned}$$

Since Barkers approximate unit impulse functions, which have constant Fourier transform, periodicities in sequence elements are represented in an optimally equal way.

A Final Thought

There is more than one way to “generalize” sequence elements.

Suppose that one proceeds from code elements represented with no decimals ($\{1, -1, i, -i\}$) and study the prevalence of Barkers as the number of decimals is increased.

The problem is still combinatorial, but there is one perhaps unexpected bit of control: at each step, exactly eight points are added to the set. (Thanks to Chris Monsour of Travellers Group for pointing this out to me).

A Last Thought, Continued

The new points come from solving for x and y in:

$$\left(\frac{x}{10^k}\right)^2 + \left(\frac{y}{10^k}\right)^2 = 1.$$

There is exactly one new solution for each increment in k, corresponding to a Pythagorean triangle with sides:

- $(n^2 - m^2)/(n^2 + m^2)$.
- $(2mn)/(n^2 + m^2)$

where:

$$\pm n \pm mi = (i^e)(1 + 2i)^k$$

and $e \in \{0, 1\}$.

A Last Thought, Continued

The new points at each step are from two symmetrically-placed points in each of the four quadrants. Here are the first several solutions:

k	x	y
0	0	1
1	0.6	0.8
2	0.28	0.96
3	0.352	0.936
4	0.5376	0.8432
5	0.0758	0.9971

(Note that using this approach, some nice properties such as the PSL-preserving operations no longer apply.)

References

[1] Borwein, P. and Ferguson, R., “Polyphase sequences with low autocorrelation”, *IEEE Transactions on Information Theory*, vol. 51 (2005), pages 1564-7.

[2] Borwein, P. and Ferguson, R., “Barker sequences”, poster session, CMS-MITACS Joint Conference 2007.

[3] Jedwab, J., “What can be used instead of a Barker sequence?”, submitted to *Contemporary Mathematics* (available at Jedwab's website).

[4] Borwein, P. and Mossinghoff, M., “Barker sequences and flat polynomials” (available at Mossinghoff's website.

[5] Jedwab, J., “A survey of the merit factor problem for binary sequences”, 23 December 2004 (available at Jedwab's website.

[6] Dmitriev, D. and Jedwab, J., “Bounds on the growth rate of the peak sidelobe level of binary sequences”, *Advances in Mathematics of Communications*.

References, Continued

[7] Barker, R., “Group synchronization of binary digital systems”, in *Communication Theory*, ed. Jackson, W., Academic Press, London, 1953.

[8] Turyn, R. and Storer, J., “On binary sequences”, *Proceedings of the AMS*, volume 12 (1961), pages 394-399.

[9] Coxson, G., “Theory of groups and low-sidelobe phase coding”, TSC noontime seminar series, 25 June 2007.

[10] Coxson, G, “Barkers beyond binary”, TSC noontime seminar series, 28 January 2008.

[11] Levanon, N., *Radar Signals*, Wiley, NY, 2005.

Additional Resources

- Ron Ferguson (Simon Fraser University, Burnaby, British Columbia)
- Idris Mercer (York University, York, Ontario).