Construction of New Asymptotic Classes of Binary Sequences Based on Existing Asymptotic Classes

Anthony Kirilusha Ganesh Narayanaswamy

July 21, 1999

Abstract

In this paper, we first demonstrate on optimally shifted Legendre sequences that an addition of a ±1 to the front of all binary sequences belonging to that class does not change the asymptotic value of the aperiodic merit factor. We then extend this result to a general case, showing that concatenation of a ±1 to the front of all sequences belonging to any asymptotic class does not affect the asymptotic merit factor value. Additionally, we present a bound on how many bits can be concatenetaded to the front before the asymptotic value becomes affected. Finally, we discuss our attempts to find classes of binary sequences with asymptotic aperiodic merit factor of 7 or greater and present a relationship between the periodic and aperiodic merit factors.

1 Introduction

1.1 Purpose

Our paper is centered around answering three main questions about binary sequences. First, is there a class of even length sequences with an asymptotic merit factor greater than 3. Second, given a class of binary sequences with a known asymptotic merit factor, how many bits can be added to the front of these sequences while still maintaining the same asymptotic merit factor. Third, does there exist a class of sequences with asymptotic merit factor greater than 6. We note that in this paper we are concerned only with the aperiodic merit factor, although some connections will be traced between the periodic and aperiodic merit factors.

1.2 Background

For consistency, let's represent our sequences of ±1's using the following notation: $S_N = x_0, x_1, \ldots, x_{N-1}$

The periodic autocorrelations of a binary sequence composed of ±1's can be defined as

$$p_k = \sum_{j=0}^{N-1} x_j x_{j+k}$$

with indices taken modulo N where N is the length of the sequence, k is the specific autocorrelation, and x_j is the value of the j^{th} term in the sequence. The k^{th} periodic autocorrelation is essentially a sum of the product of all the terms that match up between the original sequence and its cyclic offset of k places.

In general, given a sequence $S_N = x_0, x_1, \ldots, x_{N-1}$, its cyclic offset by k places can be defined as $S(k)_N = x_{0+k}, x_{1+k}, \ldots, x_{N-1+k}$ with all indeces taken modulo N. Keep in mind, that once the new indeces are computed, the x_j-th must be placed in ascending order (by the value of j) to obtain the correct sequence. For example, given $S_5 = + - - + -$, $S(2)_5 = + - + - -$.

For simplicity, we replace $+1$ with a $+$ and -1 with a $-$ when writing out sequences.

To illustrate periodic autocorrelations, let's examine $+--+-++-++-$

$$\begin{array}{ccccccccccc l}
+ & - & - & + & - & + & + & - & + & + & - & \\
- & + & - & - & + & - & + & + & - & + & + & p_1 = -5 \\
+ & - & + & - & - & + & - & + & + & - & + & p_2 = -1 \\
+ & + & - & + & - & - & + & - & + & + & - & p_3 = 7 \\
- & + & + & - & + & - & - & + & - & + & + & p_4 = -9 \\
+ & - & + & + & - & + & - & - & + & - & + & p_5 = 3 \\
+ & + & - & + & + & - & + & - & - & + & - & p_6 = 3 \\
- & + & + & - & + & + & - & + & - & - & + & p_7 = -9 \\
+ & - & + & + & - & + & + & - & + & - & - & p_8 = 7 \\
- & + & - & + & + & - & + & + & - & + & - & p_9 = -1 \\
- & - & + & - & + & + & - & + & + & - & + & p_{10} = -5
\end{array}$$

Now we will define the aperiodic autocorrelation. The k^{th} aperiodic autocorrelation coefficient of a sequence is equal to

$$c_k = \sum_{j=0}^{N-k-1} x_j x_{j+k}$$

where N is the length of the sequence and x_j is the value of the j^{th} term in the sequence. Please note that if $j > N-1$, then $x_j = 0$, since the indeces are not computed modulo N in the aperiodic case.

For example, the aperiodic autocorrelations of $+--+-++-++-$ would be

$$\begin{array}{ccccccccccc l}
+ & - & - & + & - & + & + & - & + & + & - & \\
 & + & - & - & + & - & + & + & - & + & + & c_1 = -4 \\
 & & + & - & - & + & - & + & + & - & + & c_2 = -3 \\
 & & & + & - & - & + & - & + & + & - & c_3 = 6 \\
 & & & & + & - & - & + & - & + & + & c_4 = -5 \\
 & & & & & + & - & - & + & - & + & c_5 = 0 \\
 & & & & & & + & - & - & + & - & c_6 = 3 \\
 & & & & & & & + & - & - & + & c_7 = -4 \\
 & & & & & & & & + & - & - & c_8 = 1 \\
 & & & & & & & & & + & - & c_9 = 2 \\
 & & & & & & & & & & + & c_{10} = -1
\end{array}$$

When N is odd, all the odd aperiodic autocorrelations will have an even value and all the even aperiodic autocorrelations will have an odd value. The reverse is true when N is even. Thus, at most half the aperiodic autocorrelations can be zero.

Our goal is to minimize the sum of the squares of all the autocorrelation coefficients of a sequence in order to maximize something referred to as a merit factor.

The merit factor (F_S) of a sequence, (S_N) is defined by:

$$F_S = \frac{N^2}{2\sum_{k=1}^{N-1} c_k^2}$$

In terms of power, the denominator in the formula measures the deviation of the amplitude spectrum of a transmission signal from a constant value N. Thus, small deviations would be preferred in order to ensure correct transmission. Minimizing $\sum_{k=1}^{N-1} c_k^2$ leads to maximal merit factors which is what we want. Throught this paper the term merit factor will be synonimous with the term aperiodic merit factor. The periodic variant will only be considered at the very end, and we will refer to it explicitly.

A sequence whose aperiodic autocorrelations are all either $-1, 0, 1$ is called a Barker sequence and has a maximal merit factor. For $N = 11$ and $N = 13$ there exist Barker sequences with merit factors of 12.1 and 14.08, respectively. It is conjectured that Barker sequences exist only when N is prime and $N \leq 13$. As of yet, this has not been proven, but we know that there are no Barker sequences for $13 < N < 200,000$. If this were proven to be false, then Barker sequences would be the first class of binary sequences for which the merit factor increases without bound as N tends to infinity. For now, no such classes are known to exist, although their existence is not necessarily ruled out.

We will now examine two classes of binary sequences that evolve from Hadamard difference sets. These are Legendre sequences and Modified Jacobi sequences (of which Twin-Prime sequences are a special case). Both of these classes have an asymptotic merit factor of 6 - that is, if S_N is an optimally shifted Legendre (we define what an optimum shift is later on) or a Modified Jacobi sequence of length N, then $\lim_{N\to\infty} F_S = 6$.

Legendre sequences are defined by:

$$x_i = \left(\frac{i}{p}\right) = \begin{cases} -1 & \text{if } i \text{ is a square} \pmod{p} \\ 1 & \text{if } i = 0 \text{ \& otherwise} \end{cases}$$

Example 1 *For* $N = 7$
$1^2 = 1$
$2^2 = 4$
$3^2 = 9 = 2 \pmod{7}$
$4^2 = 16 = 2 \pmod{7}$
$5^2 = 25 = 4 \pmod{7}$
$6^2 = 36 = 1 \pmod{7}$

Thus, at positions $1, 2\&4$ in the sequence there will be a -1. All the remaining positions will have a $+1$. The Legendre sequence of length 7 looks like $+--+-++$. From here on, we will refer to a Legendre sequence of length N using the notation L_N. We note that Legendre sequences are only defined for lengths N s.t. N is prime and $N \pmod 4 = 3$. Thus, there exist Legendre sequences of length 7, 11, 19, etc., but not 13, 29, and so on.

To remind the reader, a cyclic shift of a sequence is where a fraction of its elements are chopped off the end of the sequence and appended to the front. For example, for the L_7 sequence above, a cyclic shift of 2 will yield the sequence $+++--+-$ where the last two bits were chopped off and appended to the front.

A Modified Jacobi sequence of length $N = pq$ where p and q are different primes, is defined by

$$x_j = \begin{cases} \text{-1} & j = p, 2p, \ldots, (q-1)p \\ 1 & j = 0, q, 2q, \ldots, (p-1)q \\ \left(\frac{j}{N}\right) & gcd(j, N) = 1 \end{cases}$$

A special case of Modified Jacobi sequences is when $q = p + 2$, which produces a Twin-Prime sequence.

Finally, we will briefly discuss difference sets, because they are responsible for certain periodic properties of sequences based on them. Particularly, closer examination will reveal that for any L_N, all the periodic autocorrelation coefficients are equal to -1. Unfortunately, this property does not hold in the aperiodic case. A difference set is defined as follows:

Let $Z_p = \{0, 1, \ldots, p-1\}$ be a set with addition $(modp)$. Then a subset D of Z_p is a (p, k, λ) difference set (with k elements) if every nonzero element of Z_p has exactly λ solutions to $z = d_1 - d2$, $\forall (d_1, d_2) \in D$. It turns out that the positions that have value -1 in Legendre sequences form a difference set since $p \equiv 3(mod4)$. They form a $(p, (p-1)/2, (p-3)/4)$ difference set where p is the length of the sequence.

$k = (p-1)/2$ because there are $(p-1)/2$ positions that have a -1.

$\lambda = (p-3)/4$ because there are $2\binom{k}{2}$ possible non-unique solutions to $z = d_1 - d2$ $\forall (d_1, d_2) \in D$ But, for every nonzero element of Z_p, there are exactly $(2\binom{k}{2})$ solutions because there are $(p-1)$ nonzero elements in Z_p.

Since $k = (p-1)/2$,

$$\begin{aligned} \lambda &= 2((k)(k-1)/2)/(p-1) \\ &= ((p-1)/2)((p-3)/2)/(p-1) \\ &= (p-3)/4 \end{aligned}$$

According to [Hoholdt,Jensen], if F is the merit factor for an offset Legendre sequence shifted t places, as $N \rightarrow \infty$, $1/F = 2/3 - 4|f| + 8f^2, \qquad |f| \leq (1/2)$ where $|f| = t/N$

Maximizing this equation for F yields $F = 6|f| = 1/4$. This means the asymptotic merit factor for offset Legendre sequences is 6 at the optimum shifts of $\frac{1}{4} and \frac{3}{4}$ of the lengths of the sequence.

2 Concatenations

2.1 Initial Attempts

In order to create even-length sequences with good asymptotic merit factors, we initially tried a variety of methods. First we tried concatenating all possible cyclic shifts of a Legendre sequence with all the possible cyclic shifts of a Twin-Prime sequence. Since both of these classes contain only odd-length sequences, all such concatenations produced sequences of even legth. We then attempted to piece together two sequences, that is we concatenated the front of one sequence with the end of another one, ensuring that the resulting sequence is of even length. Extensive computerized searches were utilized using both of the described methods, but no hih merit factors were obtained - both techniques failed to produce sequences with merit factors above 4. We also tried to systematically improve previously constructed considering the N different codewords that are different from the original in one bit, and picking the one that has the highest merit factor. The process was repeated until changing a single bit could no longer improve the merit factor. We also tried a similar routine that changed one or two bits at a time, keeping the most beneficial switch. These procedures allowed us to improve the sequences obtained through concatenations described above, but we could see no consistent patter, and even the improved merit factors rarely exceeded 5. Our next experiment was to concatenate a ± 1 to the front of an optimally shifted Legendre sequence. This would produce an even legth sequence, and, more importantly, we had reasons to belive that as length tends to infinity, the effects of the concatenation will be less and less felt. This leads us to the discussion of our first result.

2.2 Adding ± 1 to the front of Legendre sequences

Previously, [Hoholdt,Jensen] have shown that Legendre sequences cyclically shifted by approximately $\frac{1}{4}$ of their length form a class of sequnces with an asymptotic merit factor of 6. Furthermore, since all Legendre sequences have odd lengths, addidng a ± 1 to the front of an optimally shifted Legendre sequence is a reasonable way of generating a class of even length sequences. From now on, the notation L_N, which we used to denote the actual Legendre sequence of length N, will instead imply the optimum shift of that Legendre sequence (i.e. for any length N for which a Legendre sequence is defined, we will be interested only in the shift which maximizes the merit factor). Now, let us examine what happens to the asymptotic merit factor of optimum shifts of Legendre sequences that have a +1 appended to the front. We will denote these new sequences as $1 + L_N$. First, we recall that c_k, the aperiodic autocorrelation of period k ($1 \leq k < N$, N being the length of the sequence) is defined as $\sum_{i=0}^{N-k-1} x_i x_{i+k}$ where x_i is the i-th element of the sequence, enumeration starting with 0. Appending a +1 to the front will simply add one more term to the sum, and this term will be $(1)x_k$ since the addition increases the indeces of old elements by 1. Consider the following example (we will use the shorthand + to mean a +1 and − to mean a −1): $+ - - + - + ++$ is the original Legendre sequence of length 7. For this sequence $c_2 = x_0x_2 + x_1x_3 + x_2x_4 + x_3x_5 + x_4x_6$. If we append a +1 to the front of this sequence, it will become $+(+ - - + - + ++)$ and for this longer sequence $c_2 = 1x_1 + x_0x_2 + x_1x_3 + x_2x_4 + x_3x_5 + x_4x_6$ if we use the old enumeration, or, if we renumber the sequence, every index will be increased by one and 1 will become x_0. Thus, if we call the aperiodic autocorrelations of the new sequence $c_k^{'}$, then we obtain the following expression $c_k^{'} = x_k + c_k$. Well, we know that the merit factor of a sequence, F, is defined as $\frac{N^2}{2\sum_{k=1}^{N-1}(c_k)^2}$, and it was proven by [Hoholdt,Jensen] that for Legendre sequences cyclically shifted by an optimum amount $\lim_{N\to\infty} \frac{1}{F} = \frac{1}{6}$. This implies $\lim_{N\to\infty} \frac{N^2}{2\sum_{k=1}^{N-1}(c_k)^2} = \frac{1}{6}$, so $\lim_{N\to\infty} \frac{N^2}{\sum_{k=1}^{N-1}(c_k)^2} = \frac{1}{12}$. To make our result more general, we will simply assume that there exists a class of binary sequences constructed of ±1s for which $\lim_{N\to\infty} \frac{1}{F} = 2a$, where $a > 0$ is a real constant. We therefore define the operation + on sequences to mean concatenation, and propose the following theorem:

Theorem 2 *Given a general class of sequences S_N s.t. $\lim_{N\to\infty} F_S = 2a$, $a > 0$, $a \in \Re$, and F is the aperiodic merit factor, the $\lim_{N\to\infty} F_{(1+S)} = 2a$.*

<u>Proof:</u> Let's examine what happens to the merit factor as N tends to infinity if we append a +1 in front of each sequence in the class. If we let the new merit factor be denoted as F', we have

$$F' = \frac{(N+1)^2}{2\sum_{k=1}^{N}(c_k^{'})^2} = \frac{(N+1)^2}{2\sum_{k=1}^{N}(x_k + c_k)^2} = \frac{(N+1)^2}{2(\sum_{k=1}^{N} x_k^2) + 2(\sum_{k=1}^{N} 2x_kc_k) + 2(\sum_{k=1}^{N} c_k^2)}$$

Now we can consider

$$\lim_{N\to\infty} \frac{1}{F'} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} x_k^2) + 2(\sum_{k=1}^{N} 2x_kc_k) + 2(\sum_{k=1}^{N} c_k^2)}{(N+1)^2}$$

From analysis we know that the limit of a sum is the sum of the limits provided all of them are finite. Hence, we can write

$$\lim_{N\to\infty} \frac{1}{F'} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} x_k^2)}{(N+1)^2} + \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} 2x_kc_k)}{(N+1)^2} + \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} c_k^2)}{(N+1)^2}$$

if each of the three terms converges. Well, $\lim_{N\to\infty} \frac{2(\sum_{k=1}^N x_k^2)}{(N+1)^2} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^N 1)}{(N+1)^2}$, because since x_k is ± 1, x_k^2 must equal 1. Thus

$$\lim_{N\to\infty} \frac{2(\sum_{k=1}^N x_k^2)}{(N+1)^2} = \lim_{N\to\infty} \frac{2N}{(N+1)^2} = 0$$

by the law of limits. Thereofre, the first term of our sum does converge. Now, let's examine the third term: $\lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{(N+1)^2}$. Since we assumed that $\lim_{N\to\infty} \frac{1}{F} = 2a$ for our class of sequences, we know that $\lim_{N\to\infty} \frac{2(\sum_{k=1}^{N-1} c_k^2)}{N^2} = 2a$. Also, again from analysis, we know that the limit of a product is equal to the product of the limits, provided all of them converge. We can say that

$$\lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{(N+1)^2} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{(N+1)^2 \frac{N^2}{N^2}} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{N^2} \frac{N^2}{(N+1)^2}$$

Clearly

$$\lim_{N\to\infty} \frac{N^2}{(N+1)^2} = 1$$

and

$$\lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{N^2} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N-1} c_k^2)}{N^2}$$

since $c_N = 0$ and $\lim_{N\to\infty} \frac{2(\sum_{k=1}^{N-1} c_k^2)}{N^2} = 2a$ by definition, hence

$$\lim_{N\to\infty} \frac{2(\sum_{k=1}^N c_k^2)}{(N+1)^2} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N-1} c_k^2)}{N^2} \times \lim_{N\to\infty} \frac{N^2}{(N+1)^2} = 2a \times 1 = 2a$$

which converges because a is a real constant. Finally, we should turn our attention to the second term: $\lim_{N\to\infty} \frac{2(\sum_{k=1}^N 2x_k c_k)}{(N+1)^2} = \lim_{N\to\infty} \frac{4(\sum_{k=1}^N x_k c_k)}{(N+1)^2}$. It is not immediately obvious if this limit converges or not, so to examine it, we will first solve a different problem. Suppose that given $\sum_{m=1}^n b_m^2 = d$, $d \geq 0$, $d \in \Re$, we wished to maximize $\sum_{m=1}^n b_m$. In other words, we want to maximize the sum of n elements under the constraint that the sum of their squares is some positive constant d. We can solve this problem using Lagrange multipliers: we are trying to maximize $b_1 + b_2 + ... + b_n$ knowing that $b_1^2 + b_2^2 + ... + b_n^2 = d$. First, taking the gradient of both equations yields respectively $(1, 1, ..., 1)$ and $(b_1, b_2, ..., b_n)$. To actually solve the maximization problem, we must find a λ so that

$$(1, 1, ..., 1) = \lambda(b_1, b_2, ..., b_n)$$

where $\lambda \in \Re$ is a constant. Well, the only way this is possible is if all b_m are equal to one another. Otherwise, no single constant will satisfy the expression. This implies that in order to maximize the sum $b_m = \sqrt{\frac{d}{n}}$ and leads us to the following lemma.

Lemma 3 *Given* $\sum_{m=1}^{n} b_m^2 = d$*,* $d \geq 0$*,* $d \in \Re$*, it is always true that* $\sum_{m=1}^{n} b_m \leq \sum_{m=1}^{n} \sqrt{\frac{d}{n}}$*.*

Thus armed, let's turn our attention back to the $\lim_{N\to\infty} \frac{4(\sum_{k=1}^{N} x_k c_k)}{(N+1)^2} = \lim_{N\to\infty} \frac{4(\sum_{k=1}^{N-1} x_k c_k)}{(N+1)^2}$, since $c_N = 0$. Let $\sum_{k=1}^{N-1} c_k^2 = q$. By Lemma 1

$$\sum_{k=1}^{N-1} \sqrt{c_k^2} \leq \sum_{k=1}^{N-1} \sqrt{\frac{q}{N-1}}$$

and

$$\sum_{k=1}^{N-1} \sqrt{\frac{q}{N-1}} = (N-1)\sqrt{\frac{q}{N-1}} = (N-1)(\sqrt{\frac{1}{N-1}})(\sqrt{q}) = (\sqrt{N-1})(\sqrt{q})$$

By our initial assumption $\lim_{N\to\infty} \frac{2(\sum_{k=1}^{N-1} c_k^2)}{N^2} = 2a$, so $\lim_{N\to\infty} \frac{2q}{N^2} = 2a$, which means that q is $O(N^2)$. Then $\sqrt{q}$ is $O(N)$. Furthermore, $\sqrt{N-1}$ is $O(N^{\frac{1}{2}})$, hence $(\sqrt{N-1})(\sqrt{q})$ is $O(N^{\frac{3}{2}})$. Now, consider $\sum_{k=1}^{N-1} x_k c_k$, if for every k the sign of c_k matches the sign of x_k, then $\sum_{k=1}^{N-1} x_k c_k = \sum_{k=1}^{N-1} \sqrt{c_k^2}$. Otherwise $\sum_{k=1}^{N-1} x_k c_k < \sum_{k=1}^{N-1} \sqrt{c_k^2}$. Thus

$$\lim_{N\to\infty} \frac{4(\sum_{k=1}^{N-1} x_k c_k)}{(N+1)^2} \leq \lim_{N\to\infty} \frac{4(\sum_{k=1}^{N-1} \sqrt{c_k^2})}{(N+1)^2} \leq \lim_{N\to\infty} \frac{4(\sum_{k=1}^{N-1} \sqrt{\frac{q}{N-1}})}{(N+1)^2} =$$

$$\lim_{N\to\infty} \frac{4((N-1)\sqrt{\frac{q}{N-1}})}{(N+1)^2} = \lim_{N\to\infty} \frac{4((\sqrt{N-1})(\sqrt{q}))}{(N+1)^2}$$

Since $(\sqrt{N-1})(\sqrt{q})$ is $O(N^{\frac{3}{2}})$, we can conclude that

$$\lim_{N\to\infty} \frac{4((\sqrt{N-1})(\sqrt{q}))}{(N+1)^2} = 0$$

and thus

$$\lim_{N\to\infty} \frac{4(\sum_{k=1}^{N-1} x_k c_k)}{(N+1)^2} = 0$$

Now we have shown that each term in our original sum does indeed converge to a finite value, so we can safely say that

$$\lim_{N\to\infty} \frac{1}{F'} = \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} x_k^2)}{(N+1)^2} + \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} 2x_k c_k)}{(N+1)^2} + \lim_{N\to\infty} \frac{2(\sum_{k=1}^{N} c_k^2)}{(N+1)^2}$$

and, according to the computations above,

$$\lim_{N\to\infty}\frac{1}{F'} = 0+0+2a = 2a$$

Hence

$$\lim_{N\to\infty}\frac{1}{F} = \lim_{N\to\infty}\frac{1}{F'} = 2a$$

so appending a $+1$ to the front of a sequence belonging to an asymptotic class does not alter the aperiodic merit factor as N tends to infinity. Immediately, several results follow: □

Corollary 4 *The class of even length binary sequences defined as* $1+L_N$ *has an asymptotic aperiodic merit factor of* 6*.*

Lemma 5 $\sum_{k=1}^{N-1} x_k c_k \leq \psi(N)$*, where* $\psi(N)$ *is* $O(N^{\frac{3}{2}})$*.*

Furthermore, it is quite easy to extend the argument leading to our first theorem to show that the concatenation of a -1 onto the front of a binary sequences belonging to an asymptotic class does not affect the asymptotic merit factor.

Corollary 6 *Given a general class of sequences* S_N *s.t.* $\lim_{N\to\infty} F_S = 2a$*,* $a > 0$*,* $a \in \Re$*, and* F *is the aperiodic merit factor, the* $\lim_{N\to\infty} F_{[(-1)+S]} = 2a$*.*

Proof: Going back to our initial definition of $c_k^{'}$ through c_k, we note that the only thing that will change will be that $c_k^{'} = -x_k + c_k$, so

$$F' = \frac{(N+1)^2}{2\sum_{k=1}^{N}(-x_k+c_k)^2} = \frac{(N+1)^2}{2(\sum_{k=1}^{N} x_k^2) - 2(\sum_{k=1}^{N} 2x_k c_k) + 2(\sum_{k=1}^{N} c_k^2)}$$

From there we simply retrace our original argument, except this time in order to maximize the $-4(\sum_{k=1}^{N} x_k c_k)$ we assume that $\forall\ k$, the signs of x_k and c_k are opposite. This gives us another corollary for free: □

Corollary 7 *The class of even length binary sequences defined as* $(-1)+L_N$ *has an asymptotic aperiodic merit factor of* 6*.*

2.3 Adding multiple ±1's to Legendre sequences

Since we had success adding a ±1 to the front of Next, we tried adding multiple ±1's to Legendre sequences of various lengths to see if we could still retain the asymptotic merit factor. Initially, we added $++,+-,-+,--$ to the restricted cyclic shifts of Legendre sequences and these gave consistent merit factors ≥ 5.9. The following theorem gives a bound on how many ±1's we can add to a binary sequence of length N with a known asymptotic merit factor and still retain the merit factor. The bound assumes the worst-case scenario for autocorrelation coefficients, maximizing them whenever uncertain of their value.

Theorem 8 *Let S_u be a sequence of ±1's of length u. Let S_N be a sequence of ±1's of length N that belongs to a class of sequences with a known asymptotic merit factor. Let $S_{u+N} = S_u$ concatenated with S_N. S_{u+N} will retain the asymptotic merit factor of S_N provided that $u < O(N^{1/2})$.*

Proof: For any class of sequences with an asymptotic merit factor > 0, we know

$$\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{N^2} = \lim_{N\to\infty} \frac{1}{2F_{S_N}}$$

Let S_N = sequence of ±1's of length N that belongs to a class of sequences with a known asymptotic merit factor. Suppose we add a sequence, S_u of ±1's of length u to the front of S_N, creating the sequence,S_{u+N}

$$S_{u+N} = \begin{cases} \mathrm{x}_0, \ldots, x_{u-1} & \in \mathrm{S}_u \\ \mathrm{x}_u, \ldots, x_{N+u-1} & \in \mathrm{S}_N \end{cases}$$

$c_k = k^{th}$ aperiodic autocorrelation of the original sequence, S_N
$c'_k = k^{th}$ aperiodic autocorrelation of the new sequence, S_{u+N}
The relationship between (c'_k) (c_k) is given below:

$$\begin{array}{ll} 1 \leq k \leq N-1, & c'_k = c_k + x_0x_k + x_1x_{k+1} + \cdots + x_{u-1}x_{k+u-1} \\ N \leq k \leq N+u-1, & c'_k = x_0x_k + x_1x_{k+1} + \cdots + x_{N-k-1}x_{N-1} \end{array}$$

Therefore,

$$\begin{aligned} \lim_{N\to\infty} \frac{1}{2F_{S_{u+N}}} &= \lim_{N\to\infty} \frac{\sum_{k=1}^{N+u-1}(c'_k)^2}{(N+u)^2} \\ &= \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}(c'_k)^2}{(N+u)^2} + \lim_{N\to\infty} \frac{\sum_{k=N}^{N+u-1}(c'_k)^2}{(N+u)^2} \\ &= \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}(c_k + x_0x_k + \cdots + x_{u-1}x_{k+u-1})^2}{(N+u)^2} \\ &+ \lim_{N\to\infty} \frac{\sum_{k=N}^{N+u-1}(x_0x_k + \cdots + x_{N-k-1}x_{N-1})^2}{(N+u)^2} \end{aligned}$$

First, let's deal with

$$\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}(c_k + x_0x_k + x_1x_{k+1} + \cdots + x_{u-1}x_{k+u-1})^2}{(N+u)^2} =$$

$$\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{(N+u)^2} + \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}\sum_{n=0}^{u-1} x_n^2 x_{n+k}^2}{(N+u)^2}$$

$$+ \lim_{N\to\infty} \frac{2 * \sum_{k=1}^{N-1} c_k \sum_{n=0}^{u-1} x_n x_{n+k}}{(N+u)^2} + \lim_{N\to\infty} \frac{2 * \sum_{k=1}^{N-1}\sum_{n=0}^{u-2}\sum_{m=n+1}^{u-1} x_m x_{m+k} x_n x_{n+k}}{(N+u)^2}$$

Lets's examine $\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{(N+u)^2}$

$$\begin{aligned}
\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{(N+u)^2} &= \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{(N+u)^2} \\
&= \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{\frac{(N+u)^2}{N^2} * (N^2)} \\
&= \lim_{N\to\infty} \frac{N^2}{(N+u)^2} * \lim_{N\to\infty} \frac{\sum_{k=1}^{N-1} c_k^2}{N^2} \\
&= \lim_{N\to\infty} \frac{N^2}{N^2 + 2Nu + u^2} (\lim_{N\to\infty} \frac{1}{2F_{S_N}}) \\
&= 1 * \lim_{N\to\infty} \frac{1}{2F_{S_N}} \\
&= \lim_{N\to\infty} \frac{1}{2F_{S_N}} \qquad (1)
\end{aligned}$$

provided that $u < O(N)$.

Let's examine $\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}\sum_{n=0}^{u-1} x_n^2 x_{n+k}^2}{(N+u)^2}$ We know x_n^2 & x_{n+k}^2 are both 1, $\forall(n,k)$ because x_n & x_{n+k} are either ±1. Since the inner sum runs from 0 to $u-1$, it sums up u terms (all of which are 1). Since the outer sum runs from 1 to $N-1$, it sums up N-1 terms (all of which are 1). Therefore,

$$\begin{aligned}
\lim_{N\to\infty} \frac{\sum_{k=1}^{N-1}\sum_{n=0}^{u-1} x_n^2 x_{n+k}^2}{(N+u)^2} &= \lim_{N\to\infty} \frac{(N-1)(u)}{(N+u)^2} \\
&= \lim_{N\to\infty} \frac{Nu - u}{N^2 + 2Nu + u^2} \\
&= 0 \qquad (2)
\end{aligned}$$

provided that $u < O(N)$.

Let's examine $\lim_{N\to\infty} \frac{2*\sum_{k=1}^{N-1} c_k \sum_{n=0}^{u-1} x_n x_{n+k}}{(N+u)^2}$ We want to maximize $\sum_{k=1}^{N-1} c_k \sum_{n=0}^{u-1} x_n x_{n+k}$ to find an upper bound for the limit. For the maximum sum, let's assume each product $x_n x_{n+k}$ has the same sign as c_k, $\forall\{k : 1 \leq k \leq N-1\}$. If this is the case,

$$\sum_{k=1}^{N-1} c_k \sum_{n=0}^{u-1} x_n x_{n+k} \leq \sum_{k=1}^{N-1} |c_k u|$$

$$\begin{aligned}
\lim_{N\to\infty} \frac{2*\sum_{k=1}^{N-1} c_k \sum_{n=0}^{u-1} x_n x_{n+k}}{(N+u)^2} &\leq \lim_{N\to\infty} \frac{2*\sum_{k=1}^{N-1} |c_k u|}{(N+u)^2} \\
&= 2\lim_{N\to\infty} \frac{u\sum_{k=1}^{N-1} |c_k|}{(N+u)^2} \\
&= 2\lim_{N\to\infty} \frac{u\sum_{k=1}^{N-1} + \sqrt{c_k^2}}{(N+u)^2} \\
&= 2\lim_{N\to\infty} \frac{uO(N^{3/2})}{(N+u)^2} 5 \\
&= 2\lim_{N\to\infty} \frac{uO(N^{3/2})}{N^2+2Nu+u^2} \\
&= 0
\end{aligned} \tag{3}$$

provided that $u < O(N^{1/2})$

Let's examine

$$\lim_{N\to\infty} \frac{2*\sum_{k=1}^{N-1} \sum_{n=0}^{u-2} \sum_{m=n+1}^{u-1} x_m x_{m+k} x_n x_{n+k}}{(N+u)^2}$$

To find the maximum sum, let's assume each product $x_m x_{m+k} x_n x_{n+k}$ is $+1$ ∀ (k,m,n). We know that $\sum_{n=0}^{u-2} \sum_{m=n+1}^{u-1} x_m x_{m+k} x_n x_{n+k}$ sums up $\binom{u}{2} = \frac{(u)(u-1)}{2}$ terms. Since this is only a maximum, we know

$$\begin{aligned}
\lim_{N\to\infty} \frac{2*\sum_{k=1}^{N-1} \sum_{n=0}^{u-2} \sum_{m=n+1}^{u-1} x_m x_{m+k} x_n x_{n+k}}{(N+u)^2} &\leq \lim_{N\to\infty} \frac{2(N-1)(u)(u-1)/2}{(N+u)^2} \\
&= \lim_{N\to\infty} \frac{Nu^2 - Nu - u^2 + u}{N^2+2Nu+u^2} \\
&= 0
\end{aligned} \tag{4}$$

provided that $u < O(N^{1/2})$.

From 1,2,3,4,

$$\lim_{N\to\infty}\frac{\sum_{k=1}^{N-1}(c'_k)^2}{(N+u)^2}=\lim_{N\to\infty}\frac{1}{2F_{S_N}}+0+0+0=\lim_{N\to\infty}\frac{1}{2F_{S_N}} \tag{5}$$

provided that $u < O(N^{1/2})$.

Finally, we have

$$\lim_{N\to\infty}\frac{\sum_{k=N}^{N+u-1}(x_0x_k+\cdots+x_{u-1}x_{k+u-1})^2}{(N+u)^2}$$

Since the sum

$$\sum_{k=N}^{N+u-1}(x_0x_k+\cdots+x_{u-1}x_{k+u-1})^2$$

has no c_k terms, we can maximize the sum by having every term $(x_0x_k,\ldots,x_{u-1}x_{k+u-1})$ be either 1 or -1. When $k=N$, there are u terms in the sum, when $k=N+1$, there are $u-1$ terms so on. Therefore, the sum

$$\sum_{k=N}^{N+u-1}(x_0x_k+\cdots+x_{u-1}x_{k+u-1})^2 \le (u^2+(u-1)^2+\cdots+1^2)=\frac{u(u+1)(2u+1)}{6}$$

Hence,

$$\begin{aligned}\lim_{N\to\infty}\frac{\sum_{k=N}^{N+u-1}(x_0x_k+\cdots+x_{u-1}x_{k+u-1})^2}{(N+u)^2} &\le \lim_{N\to\infty}\frac{\frac{u(u+1)(2u+1)}{6}}{(N+u)^2}\\ &= \lim_{N\to\infty}\frac{2u^3+3u^2+u}{6(N^2+2Nu+u^2)}\\ &= 0 \qquad (6)\end{aligned}$$

provided that $u < O(N^{2/3})$.

From 5,6,

$$lim_{N\to\infty}\frac{\sum_{k=1}^{N+u-1}(c'_k)^2}{(N+u)^2}=\lim_{N\to\infty}\frac{1}{2F_{S_N}}+0=\lim_{N\to\infty}\frac{1}{2F_{S_N}}$$

provided that $u < O(N^{1/2})$

$$\lim_{N\to\infty}\frac{1}{2F_{S_{u+N}}}=\lim_{N\to\infty}\frac{\sum_{k=1}^{N+u-1}(c'_k)^2}{(N+u)^2}=\lim_{N\to\infty}\frac{\sum_{k=1}^{N-1}c_k^2}{N^2}=\lim_{N\to\infty}\frac{1}{2F_{S_N}}$$

Clearly

$$\lim_{N\to\infty}F_{S_{u+N}}=\lim_{N\to\infty}F_{S_N}$$

□

We chose $u < O(\sqrt{N})$ and structured our proof to ensure that most of the terms in the sum would disappear and not affect the asymptotic behavior of our original sequence, S_N. However, as we will now see, it is possible that terms we add to the front of our sequence could be beneficial if we choose them carefully. They can be used, in some cases, to push the asymptotic merit factor above its original bound.

2.4 Observation 1

Now that we had a definite bound ($u < O(N^{1/2})$) for the number of ± 1's we could add to a class of sequences and still retain the asymptotic merit factor, we ran some computer routines to test the actual convergence of the sequence to the asymptotic bound. When using the term convergence, we are referring to the length at which the merit factor of a sequence reaches and remains above a certain value.

We ran this routine using Legendre sequences and initially set $u = \lfloor \frac{\sqrt{N}}{2} \rfloor$. Concatenating all possible sequences (S_u) of length u will all possible shifts of Legendre sequences, we looked for all concatenations that produced a merit factor ≥ 5.9. We found a convergence at $N = 127$. This meant that at all lengths at and after $N = 127$, there existed at least one concatenation, $S_{u+N} = S_u + L_N(allshifts)$, with merit factor ≥ 5.9. It turned out that for all concatenations with merit factor ≥ 5.9, S_u was exactly the same as the last u terms in L_N.

Example 9 *For* $N = 19$*,* L_N *(shifted 5)* $= ++--++-++----+-+-++$*.*
For $u = 4$*,* $S_u = +-++$*, the last 4 terms of* L_N*.*
$S_{u+N} = +-++++--++-++----+-+-++$ *of length 23*

This was an important observation, and would prove helpful in expanding the previous bound we had discovered.

Performing this concatenation with various u values, we found the following convergence values:

u − value	Convergence	AsymptoticValue
$\lfloor N^{1/3} \rfloor$	$N = 271$	6.0
$\lfloor N^{.5} \rfloor$	$N = 379$	6.2
$\lfloor N^{.55} \rfloor$	$N = 379$	6.2
$\lfloor N^{.6} \rfloor$	$N = 919$	6.2
$\lfloor N^{.63} \rfloor$	$N = 1619$	6.2
$\lfloor N^{.66} \rfloor$	$N = 1879$	6.1
$\lfloor N^{2/3} \rfloor$	$N = 2347$	6.1
$\lfloor N^{.67} \rfloor$	$N = 1699$	6.0
$\lfloor N^{.68} \rfloor$	$N = 1607$	5.9
$\lfloor N^{.7} \rfloor$	$N = 3067$	5.9

2.5 Observation 2

If we let S_u = first u terms of L_N,
$S_{N+u} = L_N + S_u$
This also gave us good merit factors for S_{N+u}.

Example 10 *For $N = 19$, L_N (shifted 5) $= ++--++-++----+-+-++$.*
For $u = 4$, $S_u = ++--$, the first 4 terms of L_N.
$S_{N+u} = ++--++-++----+-+-++++--$ *of length 23*

Performing this concatenation with various u values, we determined the following convergence values:

u − value	Convergence	AsymptoticValue
$\lfloor N^{.5} \rfloor$	$N = 379$	6.2
$\lfloor N^{.55} \rfloor$	$N = 431$	6.2
$\lfloor N^{.6} \rfloor$	$N = 2179$	6.25
$\lfloor N^{.63} \rfloor$	$N = 1699$	6.2
$\lfloor N^{2/3} \rfloor$	$N = 2411$	6.1
$\lfloor N^{.67} \rfloor$	$N = 1867$	6.0
$\lfloor N^{.7} \rfloor$	$N = 2963$	5.9

2.6 Observation 3

Up to this point, we were only working with Legendre primes that were $3 \pmod 4$. We tried to perform the above two concatenations with Legendre primes that were $1 \pmod 4$ to see if the results would be similar. Interestingly enough, when $S_u =$

last u terms of L_N, $S_{u+N} = S_u + L_N$ did not yield high merit factors.
But, when S_u = first u terms of L_N, $S_{N+u} = L_N + S_u$ did yield high merit factors.

The convergence for 1 (mod 4) primes, however, came much later than the convergence for 3 (mod 4) primes. Here are the convergence points for some u values:

u − value	Convergence	AsymptoticValue
$\lfloor N^{.5} \rfloor$	$N = 257$	5.9
$\lfloor N^{.6} \rfloor$	$N = 569$	5.9
$\lfloor N^{.63} \rfloor$	$N = 653$	5.9
$\lfloor N^{.67} \rfloor$	$N = 1549$	5.9

2.7 Discussion

Noticing these convergence values for Legendre primes both 3 (mod 4) and 1 (mod 4), we are speculating that as long as $u < O(N)$, we will get some type of convergence at some very large value of N, just by implementing the above two concatenations.

This is our conjecture based on the above data $(L_N, N \equiv 3 \pmod 4)$:

u − value	Convergence
$u < N^{.5}$	6
$N^{.5} \leq u \leq N^{2/3}$	> 6
$u > N^{2/3}$	< 6

We also ran some tests comparing F_{L_N} with $F_{S_{u+N}}$:

$N^{.5} \leq u < N^{2/3}$	$F_{S_{u+N}} > F_{L_N}$
$u = N^{2/3}$	Inconclusive
$u > N^{2/3}$	$F_{S_{u+N}} < F_{L_N}$

This also lends some credence to our conjecture. There is also a possibility that the merit factor of S_{u+N} rises and stays above 6 initially and eventually starts slowly dipping back down to 6. We do not know for certain what exactly is happening, but we do believe that it applies to Legendre sequences exclusively. We tried performing the same concatenations with Twin-Prime and Modified Jacobi sequences with no success. Therefore, we believe that some property of Legendre sequences is allowing us to concatenate part of the sequence with the entire sequence and still retain the asymptotic merit factor of 6 and even rise above 6. Our best guess, at this point, is that the aperiodic autocorrelations of the concatenated sequences are closely related to the periodic autocorrelations of Legendre sequences which are all −1.

2.8 Periodic Trends

Upon further investigation, by adding the last bits of any sequence to the front of a sequence, the aperiodic autocorrelations of the new sequence are actually related to the periodic autocorrelations (P_k) of the original sequence.

Example 11 $S_u = + - - +$
$S_N = + - + + - + - - +$
$S_{u+N} = + - - + + - + + - + - - +$

whose aperiodic autocorrelations are as follows:

$$\begin{array}{ccccccccccccccl}
+ & - & - & + & + & - & + & + & - & + & - & - & + & \\
 & + & - & - & + & + & - & + & + & - & + & - & - & c_1' = P_1 + x_0x_1 + x_1x_2 + x_2x_3 \\
 & & + & - & - & + & + & - & + & + & - & + & - & c_2' = P_2 + x_0x_2 + x_1x_3 \\
 & & & + & - & - & + & + & - & + & + & - & + & c_3' = P_3 + x_0x_3 \\
 & & & & + & - & - & + & + & - & + & + & - & c_4' = P_4 \\
 & & & & & + & - & - & + & + & - & + & + & c_5' = P_5 - x_0x_4 \\
 & & & & & & + & - & - & + & + & - & + & c_6' = P_6 - (x_0x_3 + x_1x_4) \\
 & & & & & & & + & - & - & + & + & - & c_7' = P_7 - (x_0x_2 + x_1x_3 + x_2x_4) \\
 & & & & & & & & + & - & - & + & + & c_8' = P_8 - (x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4) \\
 & & & & & & & & & + & - & - & + & c_9' = x_0x_0 + x_1x_1 + x_2x_2 + x_3x_3 = 4 \\
 & & & & & & & & & & & + & - & c_{11}' = x_0x_2 + x_1x_3 \\
 & & & & & & & & & & & & + & c_{12}' = x_0x_3
\end{array}$$

Following this pattern, we see that

$$\begin{array}{ll}
1 \le k \le u-1: & c_k' = P_k + x_0x_k + \cdots + x_{u-k-1}x_{u-1} \\
k = u: & c_k' = P_k \\
u+1 \le k \le N-1: & c_k' = P_k - (x_0x_{N-k} + \cdots + x_{k-u-1}x_{N-u-1}) \\
k = N: & c_k' = u \\
N+1 \le k \le N+u-1: & c_k' = x_0x_k + \cdots + x_{k-u-1}x_{N+u-1}
\end{array}$$

Notice that the u^{th} aperiodic autocorrelation for the new sequence is the same as the u^{th} periodic autocorrelation for the original sequence. This is due to the fact that the front u bits of the new sequence, (which are the last u bits of the original sequence) line up with the front u bits of the original sequence, causing the periodicity. Notice also that the N^{th} aperiodic autocorrelation for the new sequence has the value u. This is because the front u bits of the new sequence line up with the last u bits of the original sequence, causing each of the products to be 1. Since there are u terms lined up together, the autocorrelation value is u. In addition, we can substitute x_0 of the new sequence with x_N; x_1 with x_{N+1}; $\ldots$, x_{u-1} with x_{N+u-1} and vice versa since they are equivalent.

Another interesting observation is that

$$\begin{array}{ll} 1 \leq k \leq u-1: & c'_k = P_k + c_k(u) \\ N+1 \leq k \leq N+u-1: & c'_k = c_k(u) \end{array}$$

where $c_k(u)$ is simply the k^{th} aperiodic autocorrelation of S_u. So if we can determine something significant about this specific autocorrelation sequence, it would greatly help proving our result.

3 Conclusion

While there are several classes of binry sequences that are known to have an asymptotic merit factor of 6 (two of these classes were discussed in the introduction), we currently know of no classes s.t. $\lim_{\to\infty} F_S \geq 7$. Nevertheless, Golay proposes that the upper bound on the aperiodic merit factor is 12 as N tends to infinity, and the possibility of existence of a class of sequences for which the aperiodic merit factor increases unboundedly as N approaches infinity has not been ruled out. So far, while we have shown that given an existing asymptotic class it is easy to generate new classes with the same asymptotic merit factor, but we have been unable to find any asymptotic classes for which $\lim_{\to\infty} F_S \geq 7$. Furthermore, the relationship between the periodic and aperiodic merit factors remains unclear, although we can offer some basic explanations.

Note that for a sequence $S(N)$, $p_k = c_k + c_{N-k}$. Thus, $\sum_{k=1}^{N-1} p_k^2 = \sum_{k=1}^{N-1}(c_k + c_{N-k})^2 = 2\sum_{k=1}^{N-1} c_k^2 + 2\sum_{k=1}^{N-1} c_k c_{N-k}$.

Lemma 12 *If a, b are integers, then $a^2 + b^2 \geq 2ab$.*

<u>Proof:</u> Consider $(a-b)^2$. Clearly, $(a-b)^2 \geq 0$, hence $a^2 - 2ab + b^2 \geq 0$, thus $a^2 + b^2 \geq 2ab$. □

Then by the above lemma, $2\sum_{k=1}^{N-1} c_k c_{N-k} \leq 2\sum_{k=1}^{N-1} c_k^2$. This implies two things. First,

$$\sum_{k=1}^{N-1} p_k^2 \leq 4\sum_{k=1}^{N-1} c_k^2$$

and second

$$-\sum_{k=1}^{N-1} c_k^2 \leq \sum_{k=1}^{N-1} c_k c_{N-k} \leq \sum_{k=1}^{N-1} c_k^2$$

This representation tells us that if we have an asymptotic aperiodic class of sequences, we are guaranteed to have one with respect to the periodic merit factor as well. Also, it explains why, while the periodic merit factor of the Legendre sequences increases unboundedly as N tends to infinity, the aperiodic merit factor overs around 6. Future avenues of research may include gaining more understanding of how the term $\sum_{k=1}^{N-1} c_k c_{N-k}$ behaves under different circumstances, as well as finding new ways of generating asymtotic classes of binary sequences (with respect to the aperiodic merit factor).

4 Appendix A: Graphs of $L_N, 1 + L_N, -1 + L_N$

L_N

$1 + L_N$

$-1 + L_N$

5 Appendix B: Graphs of $S_u + L_N$

$S_u =$ last u terms of L_N

$\lfloor N^{.5} \rfloor + L_N$

$\lfloor N^{.55} \rfloor + L_N$

$\lfloor N^{.6} \rfloor + L_N$

$\lfloor N^{.63} \rfloor + L_N$

$\lfloor N^{2/3} \rfloor + L_N$

$\lfloor N^{.67} \rfloor + L_N$

6 Appendix C: Graphs of $L_N + S_u$

$S_u =$ first u terms of L_N

$L_N + \lfloor N^{.5} \rfloor$

$L_N + \lfloor N^{.55} \rfloor$

$L_N + \lfloor N^{.6} \rfloor$

$L_N + \lfloor N^{.63} \rfloor$

$L_N + \lfloor N^{2/3} \rfloor$

$L_N + \lfloor N^{.67} \rfloor$