PEAK SIDELOBE LEVEL AND PEAK CROSSCORRELATION OF GOLAY–RUDIN–SHAPIRO SEQUENCES

DANIEL J. KATZ AND COURTNEY M. VAN DER LINDEN

Abstract. Sequences with low aperiodic autocorrelation and crosscorrelation are used in communications and remote sensing. Golay and Shapiro independently devised a recursive construction that produces families of complementary pairs of binary sequences. In the simplest case, the construction produces the Rudin–Shapiro sequences, and in general it produces what we call Golay–Rudin–Shapiro sequences. Calculations by Littlewood show that the Rudin–Shapiro sequences have low mean square autocorrelation. A sequence's peak sidelobe level is its largest magnitude of autocorrelation over all nonzero shifts. Høholdt, Jensen, and Justesen showed that there is some undetermined positive constant A such that the peak sidelobe level of a Rudin–Shapiro sequence of length 2^n is bounded above by $A(1.842626\ldots)^n$, where $1.842626\ldots$ is the positive real root of X^4-3X-6. We show that the peak sidelobe level is bounded above by $5(1.658967\ldots)^{n-4}$, where $1.658967\ldots$ is the real root of X^3+X^2-2X-4. Any exponential bound with lower base will fail to be true for almost all n, and any bound with the same base but a lower constant prefactor will fail to be true for at least one n. We provide a similar bound on the peak crosscorrelation (largest magnitude of crosscorrelation over all shifts) between the sequences in each Rudin–Shapiro pair. The methods that we use generalize to all families of complementary pairs produced by the Golay–Rudin–Shapiro recursion, for which we obtain bounds on the peak sidelobe level and peak crosscorrelation with the same exponential growth rate as we obtain for the original Rudin–Shapiro sequences.

1. Introduction

Many communications and remote sensing protocols require pseudorandom sequences [Gol67,GG05,Sch09]. A *sequence* is a tuple, $(f_0, f_1, \ldots, f_{k-1})$, of complex numbers. Since we are considering aperiodic properties of sequences, we adopt the convention that $f_j = 0$ when $j \notin \{0, 1 \ldots, k-1\}$, and identify our sequence $(f_0, \ldots, f_{k-1})$ with the polynomial $f(z) = \sum_{j\in\mathbb{Z}} f_j z^j$,

Date: 13 November 2021.

This paper is based upon work supported in part by the National Science Foundation under Grants DMS-1500856 and CCF-1815487. Courtney M. van der Linden was supported in part by a Ramanujan Research Scholarship in Mathematics from the College of Science and Mathematics at California State University, Northridge.

which resides in the ring $\mathbb{C}[z, z^{-1}]$ of Laurent polynomials with complex coefficients. A *binary sequence of length* ℓ is a tuple, $(f_0, \ldots, f_{\ell-1})$, of ℓ elements from $\{1, -1\}$, that is, a polynomial $f(z) = \sum_{j \in \mathbb{Z}} f_j z^j$ where $f_j \in \{1, -1\}$ for $0 \leq j < \ell$ and $f_j = 0$ otherwise. Thus, a nonzero binary sequence of length ℓ is a polynomial of degree $\ell - 1$.

In multi-user communication networks, it is desirable to have sequences that do not resemble translates of each other, nor should any individual sequence resemble a translated version of itself [Gol67, GG05]. If f and g are two sequences and $s \in \mathbb{Z}$, then the *aperiodic crosscorrelation of* f *with* g *at shift* s is

$$C_{f,g}(s) = \sum_{j \in \mathbb{Z}} f_{j+s} \overline{g_j}. \tag{1}$$

Notice that there are only finitely many nonzero terms in this sum because our sequences have only finitely many nonzero entries. The *autocorrelation of* f *at shift* s is $C_{f,f}(s)$. We want pairs of sequences in which each sequence has low autocorrelation at all nonzero shifts and the two sequences have low crosscorrelation with each other at all shifts.

The Rudin–Shapiro sequences are family of binary sequences of increasing length, which were originally discovered by Golay [Gol51, p. 469] and Shapiro [Sha51, pp. 39–40], and later rediscovered by Rudin [Rud59, pp. 855–856]. The Rudin–Shapiro sequences are known to have low mean square autocorrelation (see [HJJ85, Theorem 2.3] or the earlier equivalent calculation in [Lit68, Problem 19]), and it has been shown [HJJ85,BM00,KLT20a,KLT20b] that relatives of the Rudin–Shapiro sequences also have low correlation. Golay devised the recursive method that produces the Rudin–Shapiro sequences and their relatives [Gol51, p. 469] in order to construct what are now called Golay complementary pairs. A *Golay complementary pair* (or *Golay pair* or *complementary pair*) is a pair of sequences (f, g) such that $C_{f,f}(s) + C_{g,g}(s) = 0$ for all nonzero $s \in \mathbb{Z}$. Shapiro's method is equivalent to Golay's, while Rudin's construction is a special case. We now formally define the recursion, which is most easily done using the polynomial interpretation of sequences.

Definition 1.1 (Golay–Rudin–Shapiro Recursion)**.** Let ℓ_0 be a positive integer and let $x_0(z)$ and $y_0(z)$ be nonzero polynomials in $\mathbb{C}[z]$ of degree less than ℓ_0 such that (x_0, y_0) is a Golay complementary pair with $C_{x_0,x_0}(0) = C_{y_0,y_0}(0)$. Let $\ell_n = 2^n \ell_0$ for each nonnegative integer n. We recursively define an infinite sequence $(x_0, y_0), (x_1, y_1), \ldots$ of pairs of polynomials where $x_n(z) = x_{n-1}(z) + z^{\ell_{n-1}} y_{n-1}(z)$ and $y_n(z) = x_{n-1}(z) - z^{\ell_{n-1}} y_{n-1}(z)$ for each $n > 0$. Then (x_n, y_n) is the *nth Golay pair obtained from* ℓ_0 *and the seed pair* (x_0, y_0) *via the Golay–Rudin–Shapiro recursion.* The sequences produced by this construction are called *Golay–Rudin–Shapiro sequences*. When one sets $\ell_0 = 1$ and $x_0(z) = y_0(z) = 1$ in this recursion, then $x_n(z)$ and $y_n(z)$ are respectively called the *nth Rudin–Shapiro sequence* and the *nth Rudin–Shapiro companion sequence*, and (x_n, y_n) is the *nth Rudin–Shapiro pair.*

Observe that x_n and y_n are polynomials of degree less than ℓ_n for each nonnegative integer n, and that they are of degree precisely $\ell_n - 1$ if $\deg(y_0) = \ell_0 - 1$, so that the nth Rudin–Shapiro sequence and its companion are binary sequences of length 2^n. For binary sequences, Golay indicates in [Gol51, p. 469] (and formally proves in [Gol61, pp. 84–85]) that each step of his construction always produces a new complementary pair from an existing one, so that every pair (x_n, y_n) produced by this construction is a complementary pair. See [KM21, Construction 6.1] for a proof that generalizes this result to work for all sequences with complex terms.

We want to investigate the correlation of Golay–Rudin–Shapiro sequences. There are two main criteria for determining how low the correlation is: a worst-case (ℓ^∞) criterion and mean square (ℓ^2) criterion. For the worst case criterion, we define the *peak crosscorrelation of sequences f and g* as

$$\mathrm{PCC}(f,g) = \max_{s\in\mathbb{Z}} |C_{f,g}(s)|,$$

and the *peak sidelobe level of f* as

$$\mathrm{PSL}(f) = \max_{s\in\mathbb{Z}\smallsetminus\{0\}} |C_{f,f}(s)|.$$

The mean square criterion is called the *demerit factor*, which gives the sum of the squared magnitudes of the correlation values over all shifts (excluding shift zero if autocorrelation is in question) when our sequences are normalized to have unit Euclidean norm. The reciprocal of a demerit factor is called a *merit factor.* The merit factor for autocorrelation was defined by Golay, who coined the term "factor" in [Gol72, p. 450], and later the full name "merit factor" in [Gol75, p. 460]. The term "demerit factor" for autocorrelation appears in the work of Sarwate [Sar84, p. 102], while for crosscorrelation, terminology both for "merit factor" and "demerit factor" appears in [Kat16, p. 5237], although mean square crosscorrelation had been studied much earlier (cf. [Sar84, eqs. (31),(38)]).

Sarwate [Sar84, eqs. (13),(38)] showed that if one randomly selects binary sequences of length ℓ, the mean autocorrelation demerit factor is $1-1/\ell$ and the mean crosscorrelation demerit factor for pairs is 1. It is known that the variance of the autocorrelation demerit factor approaches 0 as ℓ tends to infinity [BL01, pp. 1469–1470]. Thus, a randomly selected long binary sequence is very likely to have an autocorrelation demerit factor close to 1. Calculations of the L^4 norm on the complex unit circle of the associated polynomials by Littlewood [Lit68, Problem 19] show that the autocorrelation demerit factor of the Rudin–Shapiro sequences tends to $1/3$ as their length tends to infinity; this was rediscovered and explicitly realized to be a merit factor result by Høholdt, Jensen, and Justesen in [HJJ85, Theorem 2.3]. The results of Katz and Moore [KM21, Theorem 1.1] then show that the demerit factor for the crosscorrelation between a Rudin–Shapiro sequence and its companion tends to $2/3$ as the length of the sequences tends to infinity. Thus, Rudin–Shapiro sequences have significantly lower mean square autocorrelation and crosscorrelation than randomly selected binary sequences.

One should also consider how the Rudin–Shapiro sequences and their relatives rate in terms of worst-case measures of correlation (peak sidelobe level and peak crosscorrelation). In 1985, Høholdt, Jensen, and Justesen [HJJ85, p. 552] obtained a bound on the peak sidelobe level of the nth Rudin–Shapiro sequence, which we now state.

Theorem 1.2 (Høholdt–Jensen–Justesen, 1985)**.** *If n is a nonnegative integer and x_n is the nth Rudin-Shapiro sequence, then there is some $A > 0$ such that*

$$\mathrm{PSL}(x_n) \leq A(1.842626\ldots)^n,$$

where $1.842626\ldots$ *is the unique positive real root of* $X^4 - 3X - 6$.

In fact, Høholdt–Jensen–Justesen's proof works for a larger family of sequences than the Rudin–Shapiro sequences, where the extra generality comes from allowing one to choose whether or not to swap x_n and y_n with each other at each step of the recursion. Further work has been done to set lower and upper bounds on $\mathrm{PSL}(x_n)$ for the nth Rudin–Shapiro sequence, x_n, in works of Taghavi [Tag96, Tag97, Tag07] and Allouche, Choi, Denise, Erdélyi, and Saffari [ACD+19], culminating in the work of Choi [Cho20, Theorem 1.1], who gives the bound

$$0.27771487\ldots(1+o(1))\alpha_0^n \leq \mathrm{PSL}(x_n) \leq (3.78207844\ldots)\alpha_0^n,$$

where $\alpha_0 = 1.658967081916\ldots$ is the real root of $X^3 + X^2 - 2X - 4$, and the other numerical constants are approximations of numbers not explicitly defined in the theorem. In [Cho20, Theorem 1.1], there is also a bound on the crosscorrelation $C_{y_n,x_n}(s)$ values for the nth Rudin–Shapiro companion sequence y_n with the nth Rudin–Shapiro sequence x_n at shifts s with $s > 0$,

$$0.46071984\ldots(1+o(1))\alpha_0^n \leq C_{y_n,x_n}(s) \leq (3.78207844\ldots)\alpha_0^n,$$

but there is no bound for shifts $s < 0$, so we do not get a bound on $\mathrm{PCC}(y_n, x_n)$.[1]

Our Theorem 1.3 (proved as parts of Theorem 5.2 and Proposition 5.3) provides an improvement of Theorem 1.2 and all the more recent bounds on the peak sidelobe level of Rudin–Shapiro sequences.

Theorem 1.3. *If n is a nonnegative integer and x_n and y_n the nth Rudin-Shapiro sequence and its companion, then* $\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n)$, *and we have*

[1] A pair of formulae appears both in [Cho20, Theorem 1.1] and [ACD+19, Theorem 1]: $b_0 = 2 - L_n$ and $b_k = \overline{b_{-k}}$, which become $C_{y_n,x_n}(0) = 2 - 2^n$ and $C_{y_n,x_n}(k) = \overline{C_{y_n,x_n}(-k)}$ if translated into the notation of this paper. If true, these would supply the rest of the crosscorrelation values, but in fact $C_{y_n,x_n}(0) = 0$ for all $n > 1$ (see Lemma 2.12 of this paper), and the second formula has many counterexamples, e.g., $x_1 = 1 + z$ and $y_1 = 1 - z$ so that $C_{y_1,x_1}(1) = -1 \neq 1 = \overline{C_{y_1,x_1}(-1)}$, or $x_2 = 1 + z + z^2 - z^3$ and $y_2 = 1 + z - z^2 + z^3$ so that $C_{y_2,x_2}(1) = 1 \neq 3 = \overline{C_{y_2,x_2}(-1)}$.

the upper bound

$$\mathrm{PSL}(x_n) \leq 5\alpha_0^{n-4} = (0.660113\ldots)\alpha_0^n,$$

where $\alpha_0 = 1.658967\ldots$ *is the real root of* $X^3 + X^2 - 2X - 4$*. This upper bound becomes an equality if* $n = 4$*; otherwise it is a strict inequality. We also have the lower bound*

$$\mathrm{PSL}(x_n) \geq [(0.382159\ldots\ldots) - (0.421193\ldots)(0.935994\ldots)^n]\,\alpha_0^n,$$

where $0.382159\ldots = (3\alpha_0^2 + 21\alpha_0 + 2)/118$*, the quantity* $0.421193\ldots$ *is equal to* $\sqrt{(6\alpha_0^2 + 6\alpha_0 - 16)/59}$*, and* $0.935994\ldots = \sqrt{(\alpha_0^2 - 1)/2}$*.*

This shows that $0.382159\ldots \leq \limsup_{n\to\infty} \mathrm{PSL}(x_n)/\alpha_0^n \leq 0.660113\ldots$ (cf. Remark 5.4), so that one cannot lower the exponential base our upper bound without rendering it invalid for almost every n. Furthermore, if one maintains the base α_0, then the fact that the upper bound is met for $n = 4$ shows that one cannot lower its constant prefactor without rendering the bound invalid for at least one n. The lower bound in Theorem 1.3 is not very strong for small values of n. Based on computation of $\mathrm{PSL}(x_n)$ for small values of n, we also obtain (as Proposition 5.5) the following lower bound, valid for all $n > 0$ and stronger than the lower bound in Theorem 1.3 for $n \leq 42$:

$$\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n) \geq 133991557\alpha_0^{n-39} = (0.357605\ldots)\alpha_0^n,$$

with exact equality when $n = 39$, and strict inequality otherwise. The prefactor of this lower bound is more than half the prefactor of the upper bound from Theorem 1.3.

These results were obtained using a relation between the autocorrelation for the Rudin–Shapiro sequence x_n and the crosscorrelation for x_{n-1} and its companion sequence y_{n-1}. So in fact, we first proved (as parts of Theorem 5.2 and Proposition 5.3) the following analogue of Theorem 1.3 for crosscorrelation.

Theorem 1.4. *If* n *is a nonnegative integer and* x_n *and* y_n *the* n*th Rudin-Shapiro sequence and its companion, then we have the upper bound*

$$\mathrm{PCC}(x_n, y_n) \leq 5\alpha_0^{n-3} = (1.095107\ldots)\alpha_0^n,$$

where $\alpha_0 = 1.658967\ldots$ *is the real root of* $X^3 + X^2 - 2X - 4$*. This upper bound becomes an equality if* $n = 3$*; otherwise it is a strict inequality. We also have the lower bound*

$$\mathrm{PCC}(x_n, y_n) \geq [(0.633990\ldots) - (0.654022\ldots)(0.935994\ldots)^n]\,\alpha_0^n,$$

where $0.633990\ldots = (9\alpha_0^2 + 4\alpha_0 + 6)/59$*, the quantity* $0.654022\ldots$ *is equal to* $2\sqrt{(-4\alpha_0^2 + 2\alpha_0 + 14)/59}$*, and* $0.935994\ldots = \sqrt{(\alpha_0^2 - 1)/2}$*.*

As with the upper bound in Theorem 1.3, we cannot lower the exponential base of the upper bound without invalidating the bound for almost all n (see Remark 5.4), and if we maintain the base, then we cannot lower the prefactor without the bound failing for at least one n. We also have a computation-based lower bound on $\operatorname{PCC}(x_n, y_n)$ from Proposition 5.5, which is valid for all $n \in \mathbb{N}$ and stronger than the lower bound in Theorem 1.4 for $n \leq 41$:

$$\operatorname{PCC}(x_n, y_n) \geq 133991557\alpha_0^{n-38} = (0.593256\ldots)\alpha_0^n,$$

with exact equality when $n = 38$, and strict inequality otherwise. The prefactor of this lower bound is more than half the prefactor of the upper bound from Theorem 1.4.

In Theorem 5.6 (restated here as Theorem 1.5) we also prove analogous bounds for the more general class of Golay–Rudin–Shapiro sequences from Definition 1.1. To obtain a valid constant prefactor for the bounds, one needs to know the correlation values for the seed pair, (x_0, y_0), which is the origin of the recursion.

Theorem 1.5. *Suppose that n is a nonnegative integer and ℓ_n, x_n, and y_n are as in Definition 1.1, and that $K = 9\alpha_0^{-4}\operatorname{PCC}(x_0, y_0) + 18\alpha_0^{-5}\operatorname{PSL}(x_0)$, where $\alpha_0 = 1.658967\ldots$ is the real root of $X^3 + X^2 - 2X - 4$. Then $\operatorname{PCC}(x_n, y_n) \leq K\alpha_0^n$, and if $n > 0$, then $\operatorname{PSL}(x_n) = \operatorname{PSL}(y_n) \leq K\alpha_0^{n-1}$.*

As with the bounds in Theorems 1.3 and 1.4, we cannot lower the exponential base of either of these bounds without invalidating the bound for almost all n (see Remark 5.8).

This paper concerns aperiodic correlation, but here we briefly state the significance of these bounds for periodic correlation. Suppose that $f = (f_0, f_1, \ldots, f_{k-1})$ and $g = (g_0, g_1, \ldots, g_{k-1})$, and we wish these to represent periodic sequences with period k. Then for $s \in \{0, 1, \ldots, k-1\}$, the *periodic crosscorrelation of f with g*, written $\operatorname{PC}_{f,g}(s)$, equals $C_{f,g}(s) + C_{f,g}(s-k)$. In particular, note that if we are concerned with periodic autocorrelation at shift 0, then $\operatorname{PC}_{f,f}(0) = C_{f,f}(0)$, since $C_{f,f}(-k) = 0$. Since every periodic correlation is the sum of two aperiodic correlation values, we see that the periodic analogues of peak crosscorrelation and peak sidelobe level are clearly bounded above by twice the aperiodic bound:

$$\max_{0 \leq s < k} |\operatorname{PC}_{f,g}(s)| \leq 2\operatorname{PCC}(f, g)$$
$$\max_{0 < s < k} |\operatorname{PC}_{f,f}(s)| \leq 2\operatorname{PSL}(f).$$

Thus, our upper bounds from Theorems 1.3–1.5 all yield upper bounds on periodic correlation. For example, if the Rudin–Shapiro sequences x_n and y_n are regarded as sequences of period 2^n, then Theorem 1.4 shows that $\max_{0 \leq s < 2^n} |\operatorname{PC}_{x_n,y_n}(s)| \leq 10\alpha_0^{n-3}$ for every $n \in \mathbb{N}$. Since this bounding technique does not take account of possible cancellation between the two summands $C_{x_n,y_n}(s)$ and $C_{x_n,y_n}(s-2^n)$ in the expression for $\operatorname{PC}_{x_n,y_n}(s)$, our bounds on periodic correlation may not be tight, but analysis and refinement of periodic bounds is beyond the scope of this paper.

This paper is organized as follows. In Section 2, the relevant background material will be explained, including a brief exposition in Section 2.4 on how to use solely rational arithmetic to verify equations and inequalities involving the algebraic number α_0, which appears in our bounds above. In Section 2 we also begin to calculate autocorrelation and crosscorrelation of Golay–Rudin–Shapiro sequences in terms of sequences from earlier stages of the recursion. In Section 3, we iterate this recursion multiple times to obtain a bound on the crosscorrelation of our Golay pairs for the vast majority of shifts, but there is a small set of shifts for which we cannot obtain the desired bounds. We provide the results needed to close this gap in Section 4, where we prove a bound on the crosscorrelation of our Golay pairs at particular shifts that follow a special recursion. We then combine the bounds from Section 3 and Section 4 to obtain a bound for all shifts in Section 5. We use multiple methods because there does not appear to be a single technique that can be practically applied to achieve our bounds.

2. Preliminaries

In this paper, $\mathbb{N}$ denotes the set of nonnegative integers and $\mathbb{Z}^+$ denotes the set of strictly positive integers. All the definitions and notations in the Introduction remain in force for the rest of the paper. In particular, the reader should recall that we always identify a sequence $(f_0, f_1, \ldots, f_{k-1})$ of complex numbers with the polynomial $f(z) = \sum_{j\in\mathbb{Z}} f_j z^j$ using the convention that $f_j = 0$ if $j \not\in \{0, 1, \ldots, k-1\}$. Furthermore, ℓ_n, x_n, and y_n are always as specified in Definition 1.1. That is, ℓ_0 is a positive integer and x_0 and y_0 are nonzero polynomials in $\mathbb{C}[z]$ of degree less than ℓ_0 such that (x_0, y_0) is a Golay complementary pair with $C_{x_0,x_0}(0) = C_{y_0,y_0}(0)$. Also $\ell_n = 2^n\ell_0$ for each $n \in \mathbb{N}$, and we recursively define an infinite sequence of pairs $\{(x_n, y_n)\}_{n\in\mathbb{N}}$ of polynomials by the rules $x_n(z) = x_{n-1}(z) + z^{\ell_{n-1}} y_{n-1}(z)$ and $y_n(z) = x_{n-1}(z) - z^{\ell_{n-1}} y_{n-1}(z)$. That is, (x_n, y_n) is the nth Golay pair obtained from ℓ_0 and the seed pair (x_0, y_0) via the Golay–Rudin–Shapiro recursion.

2.1. **Fundamental facts.**

Throughout this paper, we let $\mathbb{C}[z, z^{-1}]$ denote the ring of Laurent polynomials with coefficients from $\mathbb{C}$. Because there is a strong connection between sequences and Laurent polynomials on the complex unit circle, if $a(z) = \sum_{j\in\mathbb{Z}} a_j z^j$, then we use $\overline{a(z)}$ as a shorthand for $\sum_{j\in\mathbb{Z}} \overline{a_j} z^{-j}$, and we also use $|a(z)|^2$ as a shorthand for $a(z)\overline{a(z)}$. The crosscorrelation of two sequences (see (1)) can be expressed as a coefficient of a particular Laurent polynomial.

Lemma 2.1. *If f and g are sequences, then*

$$f(z)\overline{g(z)} = \sum_{s\in\mathbb{Z}} C_{f,g}(s) z^s.$$

Proof. Write $f(z) = \sum_{j\in\mathbb{Z}} f_j z^j$ and $g(z) = \sum_{j\in\mathbb{Z}} g_j z^j$. The coefficient of z^s in $f(z)\overline{g(z)}$ is $\sum_{j\in\mathbb{Z}} f_{j+s}\overline{g_j}$, which is precisely $C_{f,g}(s)$. □

Corollary 2.2. *If f and g are sequences and $s \in \mathbb{Z}$, then $C_{g,f}(s) = \overline{C_{f,g}(-s)}$.*

Corollary 2.3. *If f and g are sequences, then $\operatorname{PCC}(f,g) = \operatorname{PCC}(g,f)$.*

We do not need to keep track of separate values of peak sidelobe level for the two sequences in a Golay pair, because they are always identical.

Lemma 2.4. *If (f,g) is a Golay pair, then $\operatorname{PSL}(f) = \operatorname{PSL}(g)$.*

Proof. Since (f,g) is a Golay pair, we know that $|C_{f,f}(s)| = |-C_{g,g}(s)| = |C_{g,g}(s)|$ for all nonzero $s \in \mathbb{Z}$. Therefore, $\operatorname{PSL}(f) = \operatorname{PSL}(g)$. □

2.2. **Correlation recursions.** We now prove some basic results on how the correlation values for Golay–Rudin–Shapiro sequences can be calculated from correlation values of sequences appearing in earlier stages of the recursion. First we record an important result on the degrees of our Golay–Rudin–Shapiro sequences.

Lemma 2.5. *We have $\deg(x_n), \deg(y_n) < \ell_n$ for each $n \in \mathbb{N}$. If $\deg(y_0) = \ell_0 - 1$, then $\deg(x_n) = \deg(y_n) = \ell_n - 1$ for each $n \in \mathbb{N}$. If x_0 and y_0 are binary sequences of length ℓ_0, then x_n and y_n are binary sequences of length ℓ_n for each $n \in \mathbb{N}$.*

Proof. These all follow easily by induction from the equations $\ell_n = 2^n \ell_0$, $x_n(z) = x_{n-1}(z) + z^{\ell_{n-1}} y_{n-1}(z)$, and $y_n(z) = x_{n-1}(z) - z^{\ell_{n-1}} y_{n-1}(z)$ of the Golay–Rudin–Shapiro recursion (Definition 1.1). □

In view of Lemma 2.1, the following tells us how to relate the correlation values for the pair (x_n, y_n) to those of the pair (x_{n-1}, y_{n-1}).

Lemma 2.6. *For any $n \geq 1$, we have*

$$\begin{aligned}
|x_n|^2 &= |x_{n-1}|^2 + |y_{n-1}|^2 + z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} + z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}},\\
|y_n|^2 &= |x_{n-1}|^2 + |y_{n-1}|^2 - z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} - z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}},\\
x_n\overline{y_n} &= |x_{n-1}|^2 - |y_{n-1}|^2 - z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} + z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}}, \text{ and}\\
y_n\overline{x_n} &= |x_{n-1}|^2 - |y_{n-1}|^2 + z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} - z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}}.
\end{aligned}$$

Proof. All of these are direct consequences of $x_n = x_{n-1} + z^{\ell_{n-1}} y_{n-1}$ and $y_n = x_{n-1} - z^{\ell_{n-1}} y_{n-1}$ from Definition 1.1. □

Corollary 2.7. *For each $n \in \mathbb{N}$, the pair (x_n, y_n) is a Golay complementary pair with $|x_n|^2 + |y_n|^2 = 2^n(|x_0|^2 + |y_0|^2)$, which is a constant.*

Proof. This follows by induction once one adds the first two equations of Lemma 2.6. □

Lemma 2.8. *For every $n \geq 1$, we have*

$$\begin{aligned}
|x_n|^2 &= 2^{n-1}(|x_0|^2 + |y_0|^2) + z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} + z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}}, \text{ and}\\
|y_n|^2 &= 2^{n-1}(|x_0|^2 + |y_0|^2) - z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} - z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}}.
\end{aligned}$$

For every $n \geq 2$, we have

$$\begin{aligned} x_n\overline{y_n} = z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}} - z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} \\ + 2z^{\ell_{n-2}} y_{n-2}\overline{x_{n-2}} + 2z^{-\ell_{n-2}} x_{n-2}\overline{y_{n-2}} \end{aligned} \tag{2}$$

and

$$\begin{aligned} y_n\overline{x_n} = z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} - z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}} \\ + 2z^{\ell_{n-2}} y_{n-2}\overline{x_{n-2}} + 2z^{-\ell_{n-2}} x_{n-2}\overline{y_{n-2}}. \end{aligned}$$

Proof. The first two assertions follow immediately from Lemma 2.6 and Corollary 2.7. The last two follow from the third and fourth equations of Lemma 2.6 by replacing instances of $|x_{n-1}|^2$ and $|y_{n-1}|^2$ on the right-hand sides with the expressions for $|x_{n-1}|^2$ and $|y_{n-1}|^2$ furnished by the first two equations of Lemma 2.6 (when one substitutes $n-1$ for n). □

Definition 2.9. We call the recursion in (2) the *fundamental crosscorrelation recursion.*

The following result shows that understanding the peak sidelobe levels of Golay–Rudin–Shapiro sequences is equivalent to understanding their peak crosscorrelations. In fact, we will find it more convenient to track the peak crosscorrelation and then deduce the equivalent result for peak sidelobe level.

Lemma 2.10. *For $n \in \mathbb{Z}^+$, we have* $\mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1}, y_{n-1})$.

Proof. Recall from Lemma 2.8 that we have

$$|x_n|^2 = \ell_{n-1}(|x_0|^2 + |y_0|^2) + z^{-\ell_{n-1}} x_{n-1}\overline{y_{n-1}} + z^{\ell_{n-1}} y_{n-1}\overline{x_{n-1}}.$$

To get the correlation of x_n with itself at shift s, we can read off the coefficient of z^s in this. Since $\deg x_{n-1}, \deg y_{n-1} < \ell_{n-1}$ by Lemma 2.5, the penultimate term furnishes only strictly negative powers of z (whose nonzero coefficients are the precisely the collection of nonzero crosscorrelation values for x_{n-1} with y_{n-1} by Lemma 2.1), while the final term furnishes only strictly positive powers of z (whose nonzero coefficients are precisely the collection of nonzero crosscorrelation values for y_{n-1} with x_{n-1} by Lemma 2.1), and note that $\ell_{n-1}(|x_0|^2 + |y_0|^2)$ is just a constant. Therefore,

$$\mathrm{PSL}(x_n) = \max\{\mathrm{PCC}(x_{n-1}, y_{n-1}), \mathrm{PCC}(y_{n-1}, x_{n-1})\} = \mathrm{PCC}(x_{n-1}, y_{n-1}),$$

where the second equality follows by Corollary 2.3. □

Lemma 2.11. *If $n \geq 2$, then*

$$C_{x_n,y_n}(s) = \begin{cases} \overline{C_{x_{n-1},y_{n-1}}(\ell_{n-1} - s)} + 2\overline{C_{x_{n-2},y_{n-2}}(\ell_{n-2} - s)} & \text{if } s > 0, \\ -C_{x_{n-1},y_{n-1}}(\ell_{n-1} + s) + 2C_{x_{n-2},y_{n-2}}(\ell_{n-2} + s) & \text{if } s < 0. \end{cases}$$

Proof. Suppose that $s > 0$. Read off the coefficient of z^s in the fundamental crosscorrelation recursion (2) given in Lemma 2.8. The bounds on degree in Lemma 2.5 show that positive powers of z occur only in the first and third terms of the right-hand side of (2), and then apply Corollary 2.2 to obtain the first relation. On the other hand, if $s < 0$, note that negative powers of z occur only in the second and fourth terms on the right-hand side of (2). □

In [HJJ85, Theorem 2.1] Høholdt, Jensen, and Justesen prove that the autocorrelation of any Rudin-Shapiro sequence (or its companion sequence) at a nonzero even shift is equal to zero. One has a similar result for the crosscorrelation between any Rudin-Shapiro sequence and its companion.

Lemma 2.12. *Suppose that $x_0 = y_0 = \ell_0 = 1$. Then for every $n \in \mathbb{N}$, the Laurent polynomials $|x_n|^2$, $|y_n|^2$, $x_n\overline{y_n}$, and $y_n\overline{x_n}$ have no terms of even degree, except that $|x_n|^2$ and $|y_n|^2$ have nonzero constant terms equal to 2^n, and $x_0\overline{y_0}$ and $y_0\overline{x_0}$ have nonzero constant terms equal to 1.*

Proof. One can check these statements directly for $n = 0$ and $n = 1$, and then prove the rest by induction using the formulae from Lemma 2.6. □

Remark 2.13. If we begin with $\ell_0 = 1$ and $x_0 = y_0 = 1$, then x_n and y_n are the nth Rudin–Shapiro sequence and its companion. Then $x_1 = 1 + z$ and $y_1 = 1 - z$, so one can easily calculate that $C_{x_0,y_0}(0) = 1$, $C_{x_1,y_1}(-1) = -1$, and $C_{x_1,y_1}(1) = 1$. Recall that $C_{x_n,y_n}(s) = 0$ if $|s| \geq 2^n$ (because the sequences are of length 2^n) and $C_{x_n,y_n}(s) = 0$ when $n > 0$ and s is even (by Lemma 2.12). From these facts, one can use Lemma 2.11 to compute any other value of $C_{x_n,y_n}(s)$. On Table 1, we display values of $C_{x_n,y_n}(s)$ for selected shifts s for values of $n \leq 10$. These particular values will be useful to us when we prove our bounds on peak crosscorrelation of Rudin–Shapiro sequences in Theorem 5.2. The table is constructed so that any value of $C_{x_n,y_n}(s)$ on the table with $n \geq 2$ can be obtained via Lemma 2.11 from other correlation values that are on the table (or values known from the facts stated earlier in this paragraph).

2.3. **Correlation of seed pairs.**

We record and prove some technical lemmata involving correlation values for the seed pair (x_0, y_0) in Definition 1.1. These lemmata are used in Section 5 to obtain bounds on peak crosscorrelation of all Golay pairs produced according to Definition 1.1.

Lemma 2.14. *We have $\operatorname{PCC}(x_1, y_1) \leq 2\operatorname{PSL}(x_0) + \operatorname{PCC}(x_0, y_0)$.*

Proof. Let $s \in \mathbb{Z}$. By reading the coefficient of z^s from the expression for $x_n\overline{y_n}$ in Lemma 2.6 (using $n = 1$), we see that

$$C_{x_1,y_1}(s) = C_{x_0,x_0}(s) - C_{y_0,y_0}(s) - C_{x_0,y_0}(s + \ell_0) + C_{y_0,x_0}(s - \ell_0),$$

but since x_0 and y_0 are polynomials of degree less than ℓ_0, at most one of the last two terms can be nonzero. Thus, using the triangle inequality, Corollary 2.3, and Lemma 2.4, we have $|C_{x_1,y_1}(s)| \leq 2\operatorname{PSL}(x_0) + \operatorname{PCC}(x_0, y_0)$. □

Lemma 2.15. *There is some integer s with $|s| < \ell_0$ such that $C_{x_0,y_0}(s) \neq 0$.*

Table 1. Crosscorrelation values $C_{n,s} = C_{x_n,y_n}(s)$ at selected shifts s for Rudin–Shapiro sequences x_n and their companions y_n

n	s	$C_{n,s}$	s	$C_{n,s}$	s	$C_{n,s}$	s	$C_{n,s}$	s	$C_{n,s}$
0	0	1								
1	−1	−1	1	1						
2	−3	1	−1	1	1	3	3	−1		
3	−5	−1	−3	−5	−1	3	1	1	3	1
	5	1								
4	−11	5	−7	1	−5	1	−3	5	3	7
	5	3	7	3	11	−5				
5	−21	−1	−13	−9	−11	−13	−9	3	−5	7
	5	−3	9	9	11	−7	13	5	21	1
6	−43	13	−41	−3	−27	13	−23	−7	−21	9
	−11	5	11	7	19	15	21	−5	27	7
	41	3	43	−13						
7	−85	−9	−53	−9	−45	−33	−43	−21	−23	15
	−21	−1	21	−27	23	21	37	21	43	−31
	53	5	85	9						
8	−107	53	−105	−27	−91	5	−85	49	−43	−19
	43	−1	75	15	85	−13	105	15	107	−1
	171	−21								
9	−181	−33	−171	−29	85	−83	149	−3	151	45
	171	−55	213	−19						
10	−363	109	−361	−99	−341	153	299	−57		

Proof. Since x_0 and y_0 are not zero, write $x_0 = a_h z^h + a_{h+1} z^{h+1} + \cdots + a_i z^i$ and $y_0 = b_j z^j + b_{j+1} z^{j+1} + \cdots + b_k z^k$ such that $a_i, b_j \neq 0$. Then set $s = i - j$ and note that $C_{x_0,y_0}(s)$ is the coefficient of z^{i-j} in

$$x_0 \overline{y_0} = (a_h z^h + a_{h+1} z^{h+1} + \cdots + a_i z^i)(\overline{b_k} z^{-k} + \overline{b_{k-1}} z^{-k+1} + \cdots + \overline{b_j} z^{-j}),$$

which is $a_i \overline{b_j} \neq 0$ by our assumption. Note that $0 \leq i, j < \ell_0$, so that $|s| < \ell_0$. □

Lemma 2.16. *If $\gamma \in \mathbb{C}$ with $|\gamma| \neq 1$, then there is some integer s with $|s| < \ell_0$ such that $C_{x_0,y_0}(s) \neq \gamma \overline{C_{x_0,y_0}(-s)}$.*

Proof. By Lemma 2.15, we can choose an integer t with $|t| < \ell_0$ such that $C_{x_0,y_0}(t)$ is nonzero. If $C_{x_0,y_0}(t) = \gamma \overline{C_{x_0,y_0}(-t)}$ and $C_{x_0,y_0}(-t) = \gamma \overline{C_{x_0,y_0}(-(-t))}$, then $C_{x_0,y_0}(t) = |\gamma|^2 C_{x_0,y_0}(t)$. This implies that $|\gamma| = 1$, which is a contradiction. □

2.4. **Algebraic number theory.** The bounds that we prove in this paper (Theorems 1.3–1.5) use the unique real root, α_0, of the polynomial $m(X) = X^3 + X^2 - 2X - 4 \in \mathbb{Q}[X]$. The rational roots theorem shows that this polynomial is irreducible in $\mathbb{Q}[X]$, and its discriminant is -236, so it has the single real root α_0, and two conjugate non-real roots, which we call α_1 and α_2; $m(X)$ is the minimal polynomial over $\mathbb{Q}$ of its own three roots.

It is important for us to be able to perform arithmetic in the splitting field $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ of this polynomial and to prove inequalities between pairs of real elements in this splitting field. By the irreducibility of $m(X)$, we know that $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 3$ and since $\mathbb{Q}(\alpha_0) \subseteq \mathbb{R}$, we know that $m(X)/(X - \alpha_0)$ does not factor in this field, so $[K : \mathbb{Q}(\alpha_0)] = 2$, and so $[K : \mathbb{Q}] = 6$. Then $\{\alpha_0^i : 0 \leq i < 3\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha_0)$ and $\{\alpha_0^i \alpha_1^j : 0 \leq i < 3, 0 \leq j < 2\}$ is a $\mathbb{Q}$-basis of K. Furthermore $K \cap \mathbb{R}$ is a proper subfield of K and includes $\mathbb{Q}(\alpha_0)$, but $[K : \mathbb{Q}(\alpha_0)] = 2$, so we know that $K \cap \mathbb{R} = \mathbb{Q}(\alpha_0)$. Thus, we want to know how to reduce arithmetic operations in $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ and inequalities in $K \cap \mathbb{R} = \mathbb{Q}(\alpha_0)$ to arithmetic operations and inequalities that involve only rational numbers: in this way we can use computers to assist our calculations without making any rounding errors that would compromise the certainty of our claims.

The reduction of arithmetic in an algebraic number field to rational arithmetic is well known, but we give a brief summary of an algorithm for converting any rational expression composed of elements of K into a $\mathbb{Q}$-linear combination of the $\mathbb{Q}$-basis $\{\alpha_0^i \alpha_1^j : 0 \leq i < 3, 0 \leq j < 2\}$ of K. We begin with a procedure for terms expressed as $a(\alpha_0, \alpha_1, \alpha_2)$ where $a(X, Y, Z)$ is a polynomial in $\mathbb{Q}[X, Y, Z]$. Since $m(X) = X^3 + X^2 - 2X - 4 = (X - \alpha_0)(X - \alpha_1)(X - \alpha_2)$, matching the quadratic and linear coefficients yields $\alpha_0 + \alpha_1 + \alpha_2 = -1$ and $\alpha_0(\alpha_1 + \alpha_2) + \alpha_1\alpha_2 = -2$, so that $\alpha_1 + \alpha_2 = -\alpha_0 - 1$ and $\alpha_1\alpha_2 = \alpha_0^2 + \alpha_0 - 2$. Thus, $\alpha_2 = -\alpha_0 - \alpha_1 - 1$ and $\alpha_1^2 = \alpha_1(\alpha_1 + \alpha_2) - \alpha_1\alpha_2 = \alpha_1(-\alpha_0 - 1) - (\alpha_0^2 + \alpha_0 - 2)$, and of course $\alpha_0^3 = -\alpha_0^2 + 2\alpha_0 + 4$ since α_0 is a root of $m(X)$. So given any polynomial $a(X, Y, Z) \in \mathbb{Q}[X, Y, Z]$, we can (i) replace every Z with $-X - Y - 1$ to eliminate Z, then (ii) replace any term of the form $X^i Y^j$ in which $j \geq 2$ with $X^i(-XY - Y - X^2 - X + 2)Y^{j-2}$ and keep doing so until the degree in Y is less than 2, and then (iii) replace every term $X^i Y^j$ in which $i \geq 3$ with $(-X^2 + 2X + 4)X^{i-3}Y^j$ and keep doing so until the degree in X is less than 3; we obtain a polynomial $b(X, Y) = \sum_{i=0}^{2} \sum_{j=0}^{1} b_{i,j} X^i Y^j$ with each $b_{i,j} \in \mathbb{Q}$ and with $b(\alpha_0, \alpha_1) = a(\alpha_0, \alpha_1, \alpha_2)$. This $b(X, Y)$ is called the *standard reduction* of $a(X, Y, Z)$. Since $\{\alpha_0^i \alpha_1^j : 0 \leq i < 3, 0 \leq j < 2\}$ is a $\mathbb{Q}$-basis of K and $\{\alpha_0^i : 0 \leq i < 3\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha_0) = K \cap \mathbb{R}$, we see that $b(\alpha_0, \alpha_1) \in \mathbb{R}$ if and only if Y does not appear in $b(X, Y)$.

In general, if we combine elements of K using addition, subtraction, multiplication, and division, we obtain an element $k = c(\alpha_0, \alpha_1, \alpha_2)/d(\alpha_0, \alpha_1, \alpha_2)$ for some $c(X, Y, Z)$, $d(X, Y, Z) \in \mathbb{Q}[X, Y, Z]$ with $d(\alpha_0, \alpha_1, \alpha_2) \neq 0$. Since α_1 and α_2 are conjugates, we know that $d(\alpha_0, \alpha_1, \alpha_2)d(\alpha_0, \alpha_2, \alpha_1)$ is a positive real number. So the standard reduction of $d(X, Y, Z)d(X, Z, Y)$ is some nonzero polynomial $e(X) \in \mathbb{Q}[X]$, and $k = c(\alpha_0, \alpha_1, \alpha_2)d(\alpha_0, \alpha_2, \alpha_1)/e(\alpha_0)$. Since $e(X)$ is a nonzero polynomial of degree less than 3 and $m(X)$ is cubic and irreducible over $\mathbb{Q}$, we have $\gcd(e(X), m(X)) = 1$, so the Euclidean algorithm over $\mathbb{Q}[X]$ furnishes $f(X), g(X) \in \mathbb{Q}[X]$ such that $e(X)f(X) + m(X)g(X) = 1$, so that $e(\alpha_0)f(\alpha_0) = 1$. Therefore, if we let $h(X, Y) \in$

$\mathbb{Q}[X,Y]$ be the standard reduction of $c(X,Y,Z)d(X,Z,Y)f(X)$, then $k = h(\alpha_0,\alpha_1)$. Thus, we have shown how to reduce any expression which might appear in our algebraic manipulations within $K = \mathbb{Q}(\alpha_0,\alpha_1,\alpha_2)$ to a $\mathbb{Q}$-linear combination of the $\mathbb{Q}$-basis $\{\alpha_0^i\alpha_1^j : 0 \le i < 3, 0 \le j < 2\}$ of K.

To deduce inequalities involving elements of $K \cap \mathbb{R} = \mathbb{Q}(\alpha_0)$, we compute the difference between two elements of $\mathbb{Q}(\alpha_0)$ to produce an expression of the form $v = p + q\alpha_0 + r\alpha_0^2$, where $p,q,r \in \mathbb{Q}$, and then determine whether this difference is greater than, equal to, or less than 0. We define a function that is the key to a practical algorithm for comparing v with 0.

Definition 2.17 (signifier)**.** Let $v = p + q\alpha_0 + r\alpha_0^2$ where $p,q,r \in \mathbb{Q}$. We define the *signifier of* v, written $\operatorname{sig}(v)$, to be

$$\operatorname{sig}(v) = p^3 - p^2q - 2pq^2 + 4q^3 + 5p^2r - 10pqr - 4q^2r + 12pr^2 - 8qr^2 + 16r^3.$$

Notice that the signifier is a rational number computed using solely rational arithmetic. In Proposition 2.19 below it is proved that the quantity $v = p + q\alpha_0 + r\alpha_0^2$ is zero if and only if $\operatorname{sig}(v)$ is zero, and if v and $\operatorname{sig}(v)$ are not zero, then they have the same sign. First, we prove a preliminary result.

Lemma 2.18. *Suppose that $v = p + q\alpha_0 + r\alpha_0^2$ for some $p,q,r, \in \mathbb{Q}$ with at least one of q or r nonzero. Then the minimal polynomial of v over $\mathbb{Q}$ is the cubic polynomial $n(X) = X^3 + sX^2 + tX + u$ with*

$$\begin{aligned} s &= -3p + q - 5r \\ t &= 3p^2 - 2pq - 2q^2 + 10pr - 10qr + 12r^2 \\ u &= -p^3 + p^2q + 2pq^2 - 4q^3 - 5p^2r + 10pqr + 4q^2r - 12pr^2 + 8qr^2 - 16r^3, \end{aligned}$$

and the splitting field of $n(X)$ over $\mathbb{Q}$ is K, the splitting field of $m(X) = X^3 + X^2 - 2X - 4$ over $\mathbb{Q}$, so that $n(X)$ has one real root and two conjugate non-real roots.

Proof. Since $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 3$, the set $\{1, \alpha_0, \alpha_0^2\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha_0)$, and since at least one of q or r is nonzero, this means $v \in \mathbb{Q}(\alpha_0) \smallsetminus \mathbb{Q}$. Since $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 3$, this forces v to be degree 3 over $\mathbb{Q}$, and since $\mathbb{Q}(v) \subseteq \mathbb{Q}(\alpha_0)$, this forces $\mathbb{Q}(v) = \mathbb{Q}(\alpha_0)$. We let Y be an indeterminate and set $w(Y) = p + qY + rY^2 \in \mathbb{Q}[Y]$, and then one can check that the polynomial $n(w(Y)) \in \mathbb{Q}[Y]$ can be factored as $Y^3 + Y^2 - 2Y - 4$ times $Y^3r^3 + 3Y^2qr^2 - Y^2r^3 + 3Yq^2r - 2Yqr^2 - 2Yr^3 + q^3 - q^2r - 2qr^2 + 4r^3$. So then $n(w(\alpha_0)) = 0$ because α_0 is a root of $Y^3 + Y^2 - 2Y - 4$. But $w(\alpha_0) = v$, so v is of degree 3 over $\mathbb{Q}$ and satisfies the monic cubic polynomial $n(X)$. Therefore, $n(X)$ is the minimal polynomial of v over $\mathbb{Q}$.

Let L be the splitting field of $n(X)$ over $\mathbb{Q}$. Note that $v \in \mathbb{Q}(\alpha_0) \subseteq K$, so one root of $n(X)$ lies in K. Since K is the splitting field of $m(X)$ over $\mathbb{Q}$, this means K is normal over $\mathbb{Q}$, and therefore all roots of $n(X)$ must lie in K. So $L \subseteq K$. Clearly $\mathbb{Q}(\alpha_0) = \mathbb{Q}(v) \subseteq L$. But $\mathbb{Q}(\alpha_0) = \mathbb{Q}(v)$ is not normal over $\mathbb{Q}$, because it contains the real root α_0 of $m(X)$ but does not contain the other two non-real roots of $m(X)$. So L must be strictly larger than $\mathbb{Q}(\alpha_0) = \mathbb{Q}(v)$. Since $[K : \mathbb{Q}(\alpha_0)] = 2$, this forces $L = K$. Since $n(X) \in \mathbb{Q}[x]$ and $L \not\subseteq \mathbb{R}$, one root of $n(X)$ is real and the other two are non-real conjugates. □

Proposition 2.19. *Let $v \in \mathbb{Q}(\alpha_0)$. Then $v = 0$ if and only if $\operatorname{sig}(v) = 0$, $v > 0$ if and only if $\operatorname{sig}(v) > 0$, and $v < 0$ if and only if $\operatorname{sig}(v) < 0$.*

Proof. Write $v = p + q\alpha_0 + r\alpha_0^2$ with $p, q, r \in \mathbb{Q}$. Because $\{1, \alpha_0, \alpha_0^2\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha_0)$, we know that $v \in \mathbb{Q}$ if and only if both q and r are zero. In this case, $\operatorname{sig}(v) = p^3$, and the claim is clear.

So henceforth, we assume $v \notin \mathbb{Q}$. Let $n(X) = X^3 + sX^2 + tX + u$ be the minimal polynomial over $\mathbb{Q}$ of $v \in \mathbb{Q}(\alpha_0) \setminus \mathbb{Q}$, which has only one real root by Lemma 2.18. So the graph of the function $Y = n(X)$ crosses the X-axis precisely once. Furthermore, since $n(X)$ is monic and of degree 3, if its graph crosses the X-axis at a negative X-value (i.e., the real root v is negative), then its graph crosses the Y-axis at a positive value (i.e., the constant coefficient u is positive). Similarly, if the v is positive, then u is negative. Compare u in Lemma 2.18 with $\operatorname{sig}(v)$ in Definition 2.17 to see that $-u = \operatorname{sig}(v)$, so $\operatorname{sig}(v)$ has the same the sign as v. □

We can use the signifier to produce rational approximations of real elements in $K = \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ (i.e., elements of $\mathbb{Q}(\alpha_0)$) by comparing with rational numbers. For example, we learn that $\alpha_0 = 1.658967\ldots$. We also use the signifier along with the reduction procedures detailed earlier in this section to see that α_0 is the root of $m(X) = X^3 + X^2 - 2X - 4$ with largest magnitude.

Lemma 2.20. *We have $|\alpha_1/\alpha_0| = |\alpha_2/\alpha_0| = \sqrt{(\alpha_0^2 - 1)/2} = 0.935994\ldots$.*

Proof. Since α_1 and α_2 are complex conjugates, we know that $|\alpha_1/\alpha_0|^2 = |\alpha_2/\alpha_0|^2 = \alpha_1\alpha_2/\alpha_0^2$, which can be shown to be equal to $(\alpha_0^2 - 1)/2$ by the reduction methods outlined above. One then uses the signifier methods to see that $(\alpha_0^2 - 1)/2$ lies strictly between the rational numbers 0.935994^2 and 0.935995^2. □

One consequence of this is that no nonzero power of a root of $m(X)$ can be rational.

Corollary 2.21. *If n is a nonzero integer, and $j \in \{0, 1, 2\}$, then α_j^n is irrational.*

Proof. Suppose for a contradiction that there were some nonzero integer n, some $j \in \{0, 1, 2\}$, and some $q \in \mathbb{Q}$ such that $\alpha_j^n = q$. Then since $\alpha_0, \alpha_1, \alpha_2$ are Galois conjugates over $\mathbb{Q}$, we can apply automorphisms of K over $\mathbb{Q}$ to show that $\alpha_k^n = q$ for every $k \in \{0, 1, 2\}$. In particular, this shows that α_0 and α_1 must have the same absolute value, which contradicts Lemma 2.20. □

3. Bounds from iterating the fundamental crosscorrelation recursion

In this section, we iterate the fundamental crosscorrelation recursion (2) from Lemma 2.8 multiple times to obtain formulae expressing correlation values for Golay–Rudin–Shapiro sequences in terms of correlation values of sequences appearing several steps earlier in the recursion (see Section 3.1). We then use the iterated recursive relations to deduce bounds on peak crosscorrelation of Golay pairs (see Section 3.2). These bounds are almost enough to prove via induction the main results of this paper, but there is a small interval of shifts where these bounds are not strong enough to achieve our desired bounds (see Proposition 3.7, which is proved in Section 3.3). We develop different bounds later in Section 4 to fill this gap. Recall that throughout this paper ℓ_n, x_n, y_n are always as in Definition 1.1: ℓ_0 is a positive integer and x_0 and y_0 are nonzero polynomials in $\mathbb{C}[z]$ of degree less than ℓ_0 such that (x_0, y_0) is a Golay complementary pair with $C_{x_0,x_0}(0) = C_{y_0,y_0}(0)$, and for every $n \in \mathbb{N}$, we have $\ell_n = 2^n \ell_0$ and (x_n, y_n) is the nth Golay pair obtained from ℓ_0 and the seed pair (x_0, y_0) via the Golay–Rudin–Shapiro recursion: $x_n(z) = x_{n-1}(z)+z^{\ell_{n-1}} y_{n-1}(z)$ and $y_n(z) = x_{n-1}(z)-z^{\ell_{n-1}} y_{n-1}(z)$.

3.1. **Iterating the fundamental crosscorrelation recursion.** For $t \in \mathbb{Z}^+$, we recursively define Laurent polynomials $A_t(z) = \sum_{j\in\mathbb{Z}} A_{t,j} z^j$, $B_t(z) = \sum_{j\in\mathbb{Z}} B_{t,j} z^j$, $\Gamma_t(z) = \sum_{j\in\mathbb{Z}} \Gamma_{t,j} z^j$, and $\Delta_t(z) = \sum_{j\in\mathbb{Z}} \Delta_{t,j} z^j$ by

$$\begin{aligned}
&A_1(z) = -z^{-1} && A_{t+1}(z) = -A_t(z^2) + B_t(z^2) + z\Gamma_t(z^2),\\
&B_1(z) = 1 && B_{t+1}(z) = zA_t(z^2) - zB_t(z^2) + \Delta_t(z^2),\\
&\Gamma_1(z) = 2z^{-1} && \Gamma_{t+1}(z) = 2A_t(z^2) + 2B_t(z^2),\\
&\Delta_1(z) = 2 && \Delta_{t+1}(z) = 2zA_t(z^2) + 2zB_t(z^2).
\end{aligned} \tag{3}$$

We use these Laurent polynomials to express crosscorrelations for Golay–Rudin–Shapiro sequences in terms of crosscorrelations of sequences appearing several steps earlier in the recursion. Recall from Section 2.1 that because there is a strong connection between sequences and Laurent polynomials on the complex unit circle, if $a(z) = \sum_{j\in\mathbb{Z}} a_j z^j$, then we always use $\overline{a(z)}$ as a shorthand for $\sum_{j\in\mathbb{Z}} \overline{a_j} z^{-j}$.

Proposition 3.1. *If t is a positive integer and $n > t$, then*

$$\begin{aligned}
x_n\overline{y_n} = {}& A_t(z^{\ell_{n-t+1}}) z^{2\ell_{n-t-1}} x_{n-t}\overline{y_{n-t}} + B_t(z^{\ell_{n-t+1}}) z^{2\ell_{n-t-1}} y_{n-t}\overline{x_{n-t}}\\
&+ \Gamma_t(z^{\ell_{n-t+1}}) z^{3\ell_{n-t-1}} x_{n-t-1}\overline{y_{n-t-1}} + \Delta_t(z^{\ell_{n-t+1}}) z^{\ell_{n-t-1}} y_{n-t-1}\overline{x_{n-t-1}}.
\end{aligned}$$

Proof. Proceed by induction on t. For $t = 1$ the values of A_1, B_1, Γ_1, and Δ_1 from (3) make the equation we need to prove identical to (2) from Lemma 2.8.

Now assume that the desired identity holds for some $t \geq 1$ and let $w = z^{\ell_{n-t-2}}$, so we have

$$\begin{aligned} x_n\overline{y_n} &= A_t(w^8)w^4 x_{n-t}\overline{y_{n-t}} + B_t(w^8)w^4 y_{n-t}\overline{x_{n-t}} \\ &\qquad + \Gamma_t(w^8)w^6 x_{n-t-1}\overline{y_{n-t-1}} + \Delta_t(w^8)w^2 y_{n-t-1}\overline{x_{n-t-1}}, \end{aligned} \tag{4}$$

and (2) with $n-t$ in place of n becomes

$$\begin{aligned} x_{n-t}\overline{y_{n-t}} &= w^2 y_{n-t-1}\overline{x_{n-t-1}} - w^{-2}x_{n-t-1}\overline{y_{n-t-1}} \\ &\qquad + 2(w y_{n-t-2}\overline{x_{n-t-2}} + w^{-1}x_{n-t-2}\overline{y_{n-t-2}}). \end{aligned} \tag{5}$$

Then we use (5) to replace $x_{n-t}\overline{y_{n-t}}$ and its conjugate on the right-hand side of (4) and rearrange to obtain

$$\begin{aligned} x_n\overline{y_n} &= \left(-A_t(w^8) + B_t(w^8) + w^4\Gamma_t(w^8)\right) w^2 x_{n-t-1}\overline{y_{n-t-1}} \\ &\quad + \left(w^4 A_t(w^8) - w^4 B_t(w^8) + \Delta_t(w^8)\right) w^2 y_{n-t-1}\overline{x_{n-t-1}} \\ &\quad + \left(2A_t(w^8) + 2B_t(w^8)\right) w^3 x_{n-t-2}\overline{y_{n-t-2}} \\ &\quad + \left(2w^4 A_t(w^8) + 2w^4 B_t(w^8)\right) w y_{n-t-2}\overline{x_{n-t-2}}, \end{aligned}$$

and then use the recursion in (3) to obtain the desired identity for $t+1$. □

Corollary 3.2. *Let $s \in \mathbb{Z}$ and $n, t \in \mathbb{N}$ with $0 < t < n$ and write $s = q\ell_{n-t+1} + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < \ell_{n-t+1}$. For any $m \in \mathbb{N}$ and $u \in \mathbb{Z}$, we define $C_{m,u}$ to be the coefficient of z^u in $x_m\overline{y_m}$. Then*

$$\begin{aligned} C_{n,s} &= A_{t,q}C_{n-t,r-\ell_{n-t}} + B_{t,q}\overline{C_{n-t,-r+\ell_{n-t}}} \\ &\qquad + \Gamma_{t,q}C_{n-t-1,r-3\ell_{n-t-1}} + \Delta_{t,q}\overline{C_{n-t-1,-r+\ell_{n-t-1}}}, \end{aligned}$$

Proof. We read coefficients from the formula in Proposition 3.1. First observe that $x_m\overline{y_m}$ (and its conjugate) can have nonzero coefficients for z^u only if $|u| < \ell_m$. Thus, the four terms $z^{2\ell_{n-t-1}}x_{n-t}\overline{y_{n-t}}$, $z^{2\ell_{n-t-1}}y_{n-t}\overline{x_{n-t}}$, $z^{3\ell_{n-t-1}}x_{n-t-1}\overline{y_{n-t-1}}$, and $z^{\ell_{n-t-1}}y_{n-t-1}\overline{x_{n-t-1}}$ can have nonzero coefficients for z^u only if $0 < u < \ell_{n-t+1}$. On the other hand, $A_t(z^{\ell_{n-t+1}})$, $B_t(z^{\ell_{n-t+1}})$, $\Gamma_t(z^{\ell_{n-t+1}})$, and $\Delta_t(z^{\ell_{n-t+1}})$ have nonzero coefficients only for terms z^u where u is a multiple of ℓ_{n-t+1}. So the only way to get a term with $z^s = z^{q\ell_{n-t+1}+r}$ on the right-hand side of the formula from Proposition 3.1 is to multiply the qth coefficient of A_t (resp., B_t, Γ_t, Δ_t) with the coefficient of z^r in $z^{2\ell_{n-t-1}}x_{n-t}\overline{y_{n-t}}$ (resp., $z^{2\ell_{n-t-1}}y_{n-t}\overline{x_{n-t}}$, $z^{3\ell_{n-t-1}}x_{n-t-1}\overline{y_{n-t-1}}$, $z^{\ell_{n-t-1}}y_{n-t-1}\overline{x_{n-t-1}}$), that is, with the coefficient of $z^{r-2\ell_{n-t-1}}$ (resp., the conjugate of the coefficient of $z^{-r+2\ell_{n-t-1}}$, the coefficient of $z^{r-3\ell_{n-t-1}}$, the conjugate of the coefficient of $z^{-r+\ell_{n-t-1}}$) in $x_{n-t}\overline{y_{n-t}}$ (resp., $x_{n-t}\overline{y_{n-t}}$, $x_{n-t-1}\overline{y_{n-t-1}}$, $x_{n-t-1}\overline{y_{n-t-1}}$), which is just $C_{n-t,r-\ell_{n-t}}$ (resp., $\overline{C_{n-t,-r+\ell_{n-t}}}$, $C_{n-t-1,r-3\ell_{n-t-1}}$, $\overline{C_{n-t-1,-r+\ell_{n-t-1}}}$). □

Remark 3.3. We need to compute some values of $A_{t,j}$, $B_{t,j}$, $\Gamma_{t,j}$, and $\Delta_{t,j}$ that will be critical in later proofs, and we record these values in Table 2.

For $t \in \mathbb{Z}_+$ and $j \in \mathbb{Z}$, the initial conditions from (3) tell us that

$$
\begin{aligned}
&A_{1,j} = \begin{cases} -1 & \text{if } j = -1, \\ 0 & \text{otherwise,} \end{cases} \qquad B_{1,j} = \begin{cases} 1 & \text{if } j = 0, \\ 0 & \text{otherwise,} \end{cases} \\
&\Gamma_{1,j} = \begin{cases} 2 & \text{if } j = -1, \\ 0 & \text{otherwise,} \end{cases} \qquad \Delta_{1,j} = \begin{cases} 2 & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned} \tag{6}
$$

The recursion in (3) tells us that for every $t > 0$, we have

$$
\begin{aligned}
A_{t+1,j} &= \begin{cases} -A_{t,j/2} + B_{t,j/2} & \text{if } j \text{ is even,} \\ \Gamma_{t,(j-1)/2} & \text{if } j \text{ is odd,} \end{cases} \\
B_{t+1,j} &= \begin{cases} \Delta_{t,j/2} & \text{if } j \text{ is even,} \\ A_{t,(j-1)/2} - B_{t,(j-1)/2} & \text{if } j \text{ is odd,} \end{cases} \\
\Gamma_{t+1,j} &= \begin{cases} 2A_{t,j/2} + 2B_{t,j/2} & \text{if } j \text{ is even,} \\ 0 & \text{if } j \text{ is odd,} \end{cases} \\
\Delta_{t+1,j} &= \begin{cases} 0 & \text{if } j \text{ is even,} \\ 2A_{t,(j-1)/2} + 2B_{t,(j-1)/2} & \text{if } j \text{ is odd.} \end{cases}
\end{aligned} \tag{7}
$$

The values of $A_{t,j}$, $B_{t,j}$, $\Gamma_{t,j}$, or $\Delta_{t,j}$ on Table 2 with index $t = 1$ come from (6), and those with index $t > 1$ can be computed via (7) from entries with index $t - 1$ that appear earlier on the table.

We can use Corollary 3.2 to rapidly compute crosscorrelation values. For $n, t \in \mathbb{N}$ with $0 < t < n$, we compute the crosscorrelation spectrum of the pair (x_n, y_n) from (i) the crosscorrelation spectrum of the pair (x_{n-t}, y_{n-t}), (ii) the crosscorrelation spectrum of the pair (x_{n-t-1}, y_{n-t-1}), and (iii) the values of $A_{t,q}, B_{t,q}, \Gamma_{t,q}, \Delta_{t,q}$ for $-2^{t-1} \leq q < 2^{t-1}$ (a simple inductive argument from (6) and (7) shows that $A_{t,q} = B_{t,q} = \Gamma_{t,q} = \Delta_{t,q} = 0$ for all other values of q). The number of operations it takes to compute the full crosscorrelation spectrum of (x_n, y_n) in this manner is a small multiple of $\ell_n = 2^n \ell_0$, and the number of memory locations needed to store (i) and (ii) is a small multiple of $\ell_{n-t} = 2^{n-t}\ell_0$, while the memory to store (iii) is a small multiple of of 2^t. Thus, if x_n and y_n are the Rudin–Shapiro sequences, and if we keep t around $n/2$, then the number of memory locations needed to compute the crosscorrelation spectrum for (x_n, y_n) in this manner is a small multiple of $2^{n/2}$, and the number of arithmetical operations needed is only a small multiple of the length $\ell_n = 2^n$. Since each crosscorrelation value can be computed in turn, this technique can be used to compute the peak crosscorrelation values for Golay–Rudin–Shapiro sequences that are too large to fit in the computer's memory.

Table 2. Selected Values of $A_{t,j}$, $B_{t,j}$, $\Gamma_{t,j}$, and $\Delta_{t,j}$

t	j	$A_{t,j}$	$B_{t,j}$	$\Gamma_{t,j}$	$\Delta_{t,j}$	j	$A_{t,j}$	$B_{t,j}$	$\Gamma_{t,j}$	$\Delta_{t,j}$
1	-1	-1	0	2	0	0	0	1	0	2
2	-1	2	-1	0	-2	0	1	2	2	0
3	-2	-3	-2	2	0	-1	0	3	0	2
	0	1	0	6	0	1	2	-1	0	6
4	-4	1	0	-10	0	-3	2	-1	0	-10
	1	6	1	0	2	2	-3	6	2	0
5	-6	-3	-10	2	0	2	-5	2	14	0
	4	9	0	6	0	5	2	-9	0	6
6	-12	-7	0	-26	0	-11	2	7	0	-26
	5	14	-7	0	-6	9	6	9	0	18
	10	-11	6	-14	0					
7	-23	-26	-7	0	-14	-22	5	-26	18	0
	10	-21	-6	14	0	11	0	21	0	14
	18	3	18	30	0	21	-14	-17	0	-10
8	-46	19	-14	-66	0	-43	18	31	0	-42
	21	14	-15	0	-54	37	30	-15	0	42
	42	-3	-10	-62	0					
9	-91	-66	33	0	10	-86	13	-42	98	0
	42	-29	-54	-2	0	74	-45	42	30	0
10	-182	99	10	-66	0	-181	0	-99	0	-66
	-171	98	55	0	-58	149	30	-87	0	-6

We used such techniques to compute the peak crosscorrelation for the Rudin–Shapiro sequence pairs (x_n, y_n) of length 2^n for $0 \leq n \leq 50$. The results are in Table 3: for each n it lists every shift s that yields maximum magnitude crosscorrelation, that is, every s such that $|C_{x_n,y_n}(s)| = \mathrm{PCC}(x_n, y_n)$, and for each such s, it shows the crosscorrelation value $C_{x_n,y_n}(s)$, so that one also knows the sign. Once we know about the crosscorrelation of the Rudin–Shapiro pair (x_n, y_n), then we use the first equation in Lemma 2.8 (replacing n with $n+1$) to see that for $s > 0$ we have $C_{x_{n+1},x_{n+1}}(s) = C_{y_n,x_n}(s - \ell_n) = C_{x_n,y_n}(2^n - s)$; since $C_{x_{n+1},x_{n+1}}(-s) = \overline{C_{x_{n+1},x_{n+1}}(s)}$ by Corollary 2.2, it is redundant to determine the autocorrelation at negative shifts. Proceeding in this way, we determine which positive shifts s yield maximum autocorrelation $C_{x_{n+1},x_{n+1}}(s)$, i.e., which s with $s > 0$ have $|C_{x_{n+1},x_{n+1}}(s)| = \mathrm{PSL}(x_{n+1}, x_{n+1})$. For convenience, these shifts and their corresponding autocorrelation values are shown on Table 4. It is redundant to indicate the autocorrelation values for the companion sequence, y_{n+1}, since Rudin–Shapiro pairs are Golay pairs.

3.2. **Bounds on the peak crosscorrelation.** Now we show how to use Corollary 3.2 to obtain bounds on the peak crosscorrelation of Golay–Rudin–Shapiro sequences from bounds for sequences appearing earlier in the recursion. This method almost provides an inductive proof of our bounds in Theorems 1.3–1.5, but we find that at each step there are sets of exceptional shifts for which we cannot continue the inductive chain. These exceptional

TABLE 3. Crosscorrelation values $C_{n,s} = C_{x_n,y_n}(s)$ for Rudin–Shapiro pairs, (x_n, y_n), at all shifts s such that $|C_{n,s}| = \mathrm{PCC}(x_n, y_n)$

n	s	$C_{n,s}$	s	$C_{n,s}$	n	s	$C_{n,s}$
0	0	1			26	-22369613	342769
1	-1	-1	1	1	27	-44739243	-640933
2	1	3			28	-89478451	860709
3	-3	-5			29	-178956971	-1624877
4	3	7			30	-357913941	2490985
5	-11	-13			31	-715827885	-4188609
6	13	19			32	-1431655765	7618449
7	-45	-33			33	-2863311539	-10688117
8	-107	53			34	-5726623061	20617465
9	-179	-85			35	-11453246123	-29999429
10	-341	153			36	-22906492245	51521697
11	-717	-217			37	-45812984491	-90947021
12	-1451	373			38	-91625968979	133991557
13	-2867	-557			39	-183251937963	-255886741
14	-5453	961			40	-366503875925	372089521
15	-10923	-1717			41	-733007751851	-668060317
16	-22955	2445			42	-1466015503701	1099665689
17	-43691	-4285			43	-2932031007403	-1724813029
18	-91733	6257			44	-5864062014805	3146759617
19	-174765	-11153			45	-11728124029611	-4701529197
20	-349525	19041			46	-23456248059221	8491242153
21	-699059	-28293			47	-46912496118443	-13498854709
22	-1398101	53321			48	-93824992236885	22289746385
23	-2796237	-72905			49	-187649984473771	-38672931645
24	-5592403	129485			50	-375299968947541	59901979961
25	-11184811	-214365					

sets (named E_t in Proposition 3.7 below) tend to become smaller and smaller as we iterate the fundamental crosscorrelation recursion more times (corresponding to larger t in Corollary 3.2), but we were not able to eliminate entirely these exceptional shifts after iterating many times. Therefore we deemed it impractical to attempt an inductive proof Theorems 1.3–1.5 based solely on this method of repeated iteration, and instead turned to another technique (described in Section 4) to fill in the gaps.

Notation 3.4. For the remainder of this section and for Section 3.3, the following notations, conventions and definitions are used.

- For every $k \in \mathbb{N}$, we write C_k as a shorthand for $x_k\overline{y_k}$, and we write the expansion of C_k as $C_k(z) = \sum_{j\in\mathbb{Z}} C_{k,j} z^j$.
- We let $M_k = \max_{j\in\mathbb{Z}} |C_{k,j}|$, which is just the maximum magnitude crosscorrelation between x_k and y_k, i.e., $\mathrm{PCC}(x_k, y_k)$.
- We use interval notation for subsets of $\mathbb{Z}$ rather than $\mathbb{R}$, so that (a, b) (resp., $(a, b]$, $[a, b)$, $[a, b]$) is the set of all $s \in \mathbb{Z}$ such that $a < s < b$ (resp., $a < s \leq b$, $a \leq s < b$, $a \leq s \leq b$).

TABLE 4. Autocorrelation values $D_{n,s} = C_{x_n,x_n}(s)$ for Rudin–Shapiro sequences, x_n, at all shifts $s > 0$ such that $|D_{n,s}| = \mathrm{PSL}(x_n)$

n	s	$D_{n,s}$	s	$D_{n,s}$	n	s	$D_{n,s}$
0	all $s > 0$	0			26	44739243	-214365
1	1	1			27	89478477	342769
2	1	1	3	-1	28	178956971	-640933
3	3	3			29	357913907	860709
4	11	-5			30	715827883	-1624877
5	13	7			31	1431655765	2490985
6	43	-13			32	2863311533	-4188609
7	51	19			33	5726623061	7618449
8	173	-33			34	11453246131	-10688117
9	363	53			35	22906492245	20617465
10	691	-85			36	45812984491	-29999429
11	1365	153			37	91625968981	51521697
12	2765	-217			38	183251937963	-90947021
13	5547	373			39	366503875923	133991557
14	11059	-557			40	733007751851	-255886741
15	21837	961			41	1466015503701	372089521
16	43691	-1717			42	2932031007403	-668060317
17	88491	2445			43	5864062014805	1099665689
18	174763	-4285			44	11728124029611	-1724813029
19	353877	6257			45	23456248059221	3146759617
20	699053	-11153			46	46912496118443	-4701529197
21	1398101	19041			47	93824992236885	8491242153
22	2796211	-28293			48	187649984473771	-13498854709
23	5592405	53321			49	375299968947541	22289746385
24	11184845	-72905			50	750599937895083	-38672931645
25	22369619	129485			51	1501199875790165	59901979961

- If $S \subseteq \mathbb{Z}$ and c is a positive integer, we write $S \cdot c$ to mean $\{sc : s \in S\}$. For example, $((1,2] \cup (3,4)) \cdot c = (c, 2c] \cup (3c, 4c)$.

Now we use Corollary 3.2 to produce general bounds on peak crosscorrelation.

Lemma 3.5. *Let $n, t \in \mathbb{N}$ with $0 < t < n$, let $s \in \mathbb{Z}$, and write $s = q\ell_{n-t+1} + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < \ell_{n-t+1}$. Then*

$$|C_{n,s}| \leq \begin{cases} (|A_{t,q}| + |B_{t,q}|)M_{n-t} + |\Delta_{t,q}|M_{n-t-1} & \text{if } 0 < r < \ell_{n-t}, \\ (|A_{t,q}| + |B_{t,q}|)M_{n-t} + |\Gamma_{t,q}|M_{n-t-1} & \text{if } \ell_{n-t} < r < \ell_{n-t+1}, \\ (|A_{t,q}| + |B_{t,q}|)M_{n-t} & \text{if } r = \ell_{n-t}, \end{cases}$$

and $C_{n,s} = 0$ if $r = 0$.

Proof. By Corollary 3.2, the coefficient of z^s in $x_n\overline{y_n}$ is

$$\begin{aligned} C_{n,s} = A_{t,q}C_{n-t,r-\ell_{n-t}} + B_{t,q}\overline{C_{n-t,\ell_{n-t}-r}} \\ + \Gamma_{t,q}C_{n-t-1,r-3\cdot\ell_{n-t-1}} + \Delta_{t,q}\overline{C_{n-t-1,\ell_{n-t-1}-r}}. \end{aligned} \tag{8}$$

If $r = 0$, then we cannot get a contribution from any of the four terms, since the shift for that term is larger in magnitude than the degrees of the sequences being correlated (cf. Lemma 2.5), and so $C_{n,s} = 0$. Likewise, if $0 < r \leq \ell_{n-t}$, we cannot get a contribution from $C_{n-t-1,r-3\cdot\ell_{n-t-1}}$, while if $\ell_{n-t} \leq r < \ell_{n-t+1}$, we cannot get a contribution from $\overline{C_{n-t-1,\ell_{n-t-1}-r}}$. We prove the bounds for the three cases by dropping these non-contributory terms from (8), then taking absolute values of both sides, using the triangle inequality on the right-hand side, and bounding the absolute value of each specific correlation value $C_{k,u}$ with its largest possible magnitude M_k. □

The following technical result gives bounds on crosscorrelations for our Golay pairs (x_n, y_n) in terms of the crosscorrelation and autocorrelation of the seed pair (x_0, y_0), and is used in establishing the constant prefactor in the bound of Theorem 1.5.

Lemma 3.6. *If $s \in \mathbb{Z}$, $n \in \mathbb{Z}_+$, and $q = \lfloor s/\ell_2 \rfloor$, then*

$$|C_{x_n,y_n}(s)| \leq \big(|A_{n-1,q}| + |B_{n-1,q}| + |\Gamma_{n-1,q}| + |\Delta_{n-1,q}|\big) \cdot \mathrm{PCC}(x_0, y_0) \\ + \big(|A_{n-1,q}| + |B_{n-1,q}|\big) \cdot 2\,\mathrm{PSL}(x_0).$$

Proof. Apply Lemma 3.5 with $t = n - 1$ (noting that q as defined here is the same q as in the lemma) to see that

$$|C_{n,s}| \leq (|A_{n-1,q}| + |B_{n-1,q}|)M_1 + (|\Delta_{n-1,q}| + |\Gamma_{n-1,q}|)M_0,$$

and then note that $M_0 = \mathrm{PCC}(x_0, y_0)$ and Lemma 2.14 says that $M_1 = \mathrm{PCC}(x_1, y_1) \leq 2\,\mathrm{PSL}(x_0) + \mathrm{PCC}(x_0, y_0)$. □

3.3. **Inductive bounds.** Recall the algebraic number α_0, which appears in our bounds in Theorems 1.3–1.5, and whose technical details are described in Section 2.4. We show that if we have established an exponential bound with base α_0 for crosscorrelation of Golay–Rudin–Shapiro sequences appearing earlier in the recursion, then in most cases we can deduce such a bound for Golay–Rudin–Shapiro sequences appearing later in the recursion, but this does not amount to a full inductive proof because there are exceptional sets of shifts (called E_t in the result below) for which the inductive chain does not continue.

Proposition 3.7. *Let $n \in \mathbb{N}$ and suppose that there is some positive real number K such that for all $m < n$ we have $\mathrm{PCC}(x_m) \leq K\alpha_0^m$. For each $t \in \{1, 2, \ldots, 10\}$, define E_t by*

(1) $E_1 = (-1, 1) \cdot \ell_{n-1}$,
(2) $E_2 = (-2, 2) \cdot \ell_{n-2}$,
(3) $E_3 = \big((-4, -2) \cup (1, 3)\big) \cdot \ell_{n-3}$,
(4) $E_4 = \big([-6, -5) \cup (2, 3) \cup [4, 6)\big) \cdot \ell_{n-4}$,
(5) $E_5 = \big([-12, -10) \cup (5, 6) \cup (9, 11)\big) \cdot \ell_{n-5}$,
(6) $E_6 = \big((-23, -21) \cup (10, 12) \cup (18, 19) \cup (21, 22)\big) \cdot \ell_{n-6}$,
(7) $E_7 = \big((-46, -45) \cup (-43, -42) \cup (21, 22) \cup (37, 38) \cup (42, 43)\big) \cdot \ell_{n-7}$,

(8) $E_8 = \big((-91,-90) \cup (-86,-85) \cup (42,43) \cup (74,75)\big) \cdot \ell_{n-8}$,
(9) $E_9 = \big((-182,-180) \cup (-171,-170) \cup (149,150)\big) \cdot \ell_{n-9}$, *and*
(10) $E_{10} = (-342,-341) \cdot \ell_{n-10}$.

Then for each $t \in \{1,\ldots,10\}$*, if* $n > t$ *and* $s \notin E_t$*, then* $|C_{n,s}| \leq K\alpha_0^n$*.*

Proof. Set $E_0 = (-\ell_n, \ell_n)$. When we prove the $t = 1$ case, we may confine ourselves to $s \in E_0$, since otherwise $C_{n,s} = 0$ (because $\deg x_n, \deg y_n < \ell_n$ by Lemma 2.5). For each $t \in \{1,\ldots,10\}$, define $F_t = E_{t-1} \smallsetminus E_t$. Since we prove cases with $t = 1,2,\ldots,10$ in ascending order, the tth instance needs only be shown for $s \in F_t$. We work out what the sets $F_1,\ldots,F_{10}$ are:

(1) $F_1 = \big((-2,-1] \cup [1,2)\big) \cdot \ell_{n-1}$,
(2) $F_2 = \emptyset$,
(3) $F_3 = \big([-2,1] \cup [3,4)\big) \cdot \ell_{n-3}$,
(4) $F_4 = \big((-8,-6) \cup [-5,-4) \cup [3,4)\big) \cdot \ell_{n-4}$,
(5) $F_5 = \big((4,5] \cup [8,9] \cup [11,12)\big) \cdot \ell_{n-5}$,
(6) $F_6 = \big([-24,-23] \cup [-21,-20) \cup [19,21]\big) \cdot \ell_{n-6}$,
(7) $F_7 = \big([-45,-43] \cup (20,21] \cup [22,24) \cup (36,37] \cup [43,44)) \cdot \ell_{n-7}$,
(8) $F_8 = \big((-92,-91] \cup [-85,-84) \cup [43,44) \cup [75,76) \cup (84,86)\big) \cdot \ell_{n-8}$,
(9) $F_9 = \big((-172,-171] \cup (84,86) \cup (148,149]\big) \cdot \ell_{n-9}$, and
(10) $F_{10} = \big((-364,-360) \cup [-341,-340) \cup (298,300)\big) \cdot \ell_{n-10}$.

Now we write $s \in F_t$ as $s = q \cdot \ell_{n-t+1} + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < \ell_{n-t+1}$. For each value of t, we give all the possibilities for q and r, arranged into subcases.

(1) For $t = 1$, we have $q = -1$ and $r \in (0, \ell_{n-1}]$; or $q = 0$ and $r \in [\ell_{n-1}, \ell_n)$.
(2) For $t = 2$, there is nothing to prove.
(3) For $t = 3$, we have $q = -1$ and $r \in [0, \ell_{n-3})$; or $q = 1$ and $r \in [\ell_{n-3}, \ell_{n-2})$.
(4) For $t = 4$, we have $q = -4$ and $r \in (0, \ell_{n-3})$; $q = -3$ and $r \in [\ell_{n-4}, \ell_{n-3})$; or $q = 1$ and $r \in [\ell_{n-4}, \ell_{n-3})$.
(5) For $t = 5$, we have $q = 2$ and $r \in (0, \ell_{n-5}]$; $q = 4$ and $r \in [0, \ell_{n-5}]$; or $q = 5$ and $r \in [\ell_{n-5}, \ell_{n-4})$.
(6) For $t = 6$, we have $q = -12$ and $r \in [0, \ell_{n-6}]$; $q = -11$ and $r \in [\ell_{n-6}, \ell_{n-5})$; $q = 9$ and $r \in [\ell_{n-6}, \ell_{n-5})$; or $q = 10$ and $r \in [0, \ell_{n-6}]$.
(7) For $t = 7$, we have $q = -23$ and $r \in [\ell_{n-7}, \ell_{n-6})$; $q = -22$ and $r \in [0, \ell_{n-7}]$; $q = 10$ and $r \in (0, \ell_{n-7}]$; $q = 11$ and $r \in [0, \ell_{n-6})$; $q = 18$ and $r \in (0, \ell_{n-7}]$; or $q = 21$ and $r \in [\ell_{n-7}, \ell_{n-6})$.
(8) For $t = 8$, we have $q = -46$ and $r \in (0, \ell_{n-8}]$; $q = -43$ and $r \in [\ell_{n-8}, \ell_{n-7})$; $q = 21$ and $r \in [\ell_{n-8}, \ell_{n-7})$; $q = 37$ and $r \in [\ell_{n-8}, \ell_{n-7})$; or $q = 42$ and $r \in (0, \ell_{n-7})$.
(9) For $t = 9$, we have $q = -86$ and $r \in (0, \ell_{n-9}]$; $q = 42$ and $r \in (0, \ell_{n-8})$; or $q = 74$ and $r \in (0, \ell_{n-9}]$.

(10) For $t = 10$, we have $q = -182$ and $r \in (0, \ell_{n-9})$; $q = -181$ and $r \in [0, \ell_{n-9})$; $q = -171$ and $r \in [\ell_{n-10}, \ell_{n-9})$; or $q = 149$ and $r \in (0, \ell_{n-9})$.

Then for each value of t, and for each specified q and range of values of r that we have listed for that t, we use the appropriate case of Lemma 3.5 with values of $A_{t,q}$, $B_{t,q}$, $\Gamma_{t,q}$, and $\Delta_{t,q}$ from Table 2 to give a bound on $|C_{n,s}|$ where $s = q \cdot \ell_n + r$. The bounds we get for each value of t (considering all of its subcases listed above) are as follows.

(1) For $t = 1$, our two subcases give $|C_{n,s}| \leq M_{n-1}$; or $|C_{n,s}| \leq M_{n-1}$.
(2) For $t = 2$, there is nothing to prove.
(3) For $t = 3$, our two subcases give $|C_{n,s}| \leq 3M_{n-3}+2M_{n-4}$; or $|C_{n,s}| \leq 3M_{n-3}$.
(4) For $t = 4$, our three subcases give $|C_{n,s}| \leq M_{n-4} + 10M_{n-5}$; $|C_{n,s}| \leq 3M_{n-4}$; or $|C_{n,s}| \leq 7M_{n-4}$.
(5) For $t = 5$, our three subcases give $|C_{n,s}| \leq 7M_{n-5}$; $|C_{n,s}| \leq 9M_{n-5}$; or $|C_{n,s}| \leq 11M_{n-5}$.
(6) For $t = 6$, our four subcases give $|C_{n,s}| \leq 7M_{n-6}$; $|C_{n,s}| \leq 9M_{n-6}$; $|C_{n,s}| \leq 15M_{n-6}$; or $|C_{n,s}| \leq 17M_{n-6}$.
(7) For $t = 7$, our six subcases give $|C_{n,s}| \leq 33M_{n-7}$; $|C_{n,s}| \leq 31M_{n-7}$; $|C_{n,s}| \leq 27M_{n-7}$; $|C_{n,s}| \leq 21M_{n-7} + 14M_{n-8}$; $|C_{n,s}| \leq 21M_{n-7}$; or $|C_{n,s}| \leq 31M_{n-7}$.
(8) For $t = 8$, our five subcases give $|C_{n,s}| \leq 33M_{n-8}$; $|C_{n,s}| \leq 49M_{n-8}$; $|C_{n,s}| \leq 29M_{n-8}$; $|C_{n,s}| \leq 45M_{n-8}$; or $|C_{n,s}| \leq 13M_{n-8} + 62M_{n-9}$.
(9) For $t = 9$, our three subcases give $|C_{n,s}| \leq 55M_{n-9}$; $|C_{n,s}| \leq 83M_{n-9} + 2M_{n-10}$; or $|C_{n,s}| \leq 87M_{n-9}$.
(10) For $t = 10$, our four subcases give $|C_{n,s}| \leq 109M_{n-10} + 66M_{n-11}$; $|C_{n,s}| \leq 99M_{n-10} + 66M_{n-11}$; $|C_{n,s}| \leq 153M_{n-10}$; or $117M_{n-10} + 6M_{n-11}$.

Now by our hypothesis that $M_j \leq K\alpha_0^j$ for all $j < n$, so for each of the cases we know that if $s \in F_t$, then we have the following.

(1) If $t = 1$, then $|C_{n,s}| \leq K\alpha_0^{n-1}$.
(2) If $t = 2$, then nothing needs to be proved.
(3) If $t = 3$, then $|C_{n,s}| \leq 3K\alpha_0^{n-3} + 2K\alpha_0^{n-4}$.
(4) If $t = 4$, then $|C_{n,s}| \leq \max\{K\alpha_0^{n-4} + 10K\alpha_0^{n-5}, 7K\alpha_0^{n-4}\}$.
(5) If $t = 5$, then $|C_{n,s}| \leq 11K\alpha_0^{n-5}$.
(6) If $t = 6$, then $|C_{n,s}| \leq 17K\alpha_0^{n-6}$.
(7) If $t = 7$, then $|C_{n,s}| \leq \max\{33K\alpha_0^{n-7}, 21K\alpha_0^{n-7} + 14K\alpha_0^{n-8}\}$.
(8) If $t = 8$, then $|C_{n,s}| \leq \max\{49K\alpha_0^{n-8}, 13K\alpha_0^{n-8} + 62K\alpha_0^{n-9}\}$.
(9) If $t = 9$, then $|C_{n,s}| \leq \max\{87K\alpha_0^{n-9}, 83K\alpha_0^{n-9} + 2K\alpha_0^{n-10}\}$.
(10) If $t = 10$, then $|C_{n,s}| \leq \max\{109K\alpha_0^{n-10} + 66K\alpha_0^{n-11}, 153K\alpha_0^{n-10}, 117K\alpha_0^{n-10} + 6K\alpha_0^{n-11}\}$.

Then one must show that these upper bounds are less than or equal to $K\alpha_0^n$, which one does by dividing the above bound for the tth case by $K\alpha_0^{n-t-1}$

and showing that this quotient is less than α_0^{t+1}. For example, if $t = 7$, we must show that $33\alpha_0 \leq \alpha_0^8$ and $21\alpha_0 + 14 \leq \alpha_0^8$. Section 2.4 shows how to verify such inequalities using purely rational arithmetic. □

4. Correlations for recursive shifts

In the last section, we iterated the fundamental crosscorrelation recursion (2) from Lemma 2.8 many times in an attempt to provide an inductive proof of Theorems 1.3–1.5, but we found that there were exceptional shifts for which the induction could not be continued. This section provides another inductive argument that also fails to work for some shifts, but will be shown to work for the critical shifts for which the method of Section 3 fails.

Recall that throughout this paper ℓ_n, x_n, y_n are always as in Definition 1.1: ℓ_0 is a positive integer and x_0 and y_0 are nonzero polynomials in $\mathbb{C}[z]$ of degree less than ℓ_0 such that (x_0, y_0) is a Golay complementary pair with $C_{x_0,x_0}(0) = C_{y_0,y_0}(0)$, and for every $n \in \mathbb{N}$, we have $\ell_n = 2^n\ell_0$ and (x_n, y_n) is the nth Golay pair obtained from ℓ_0 and the seed pair (x_0, y_0) via the Golay–Rudin–Shapiro recursion: $x_n(z) = x_{n-1}(z) + z^{\ell_{n-1}}y_{n-1}(z)$ and $y_n(z) = x_{n-1}(z) - z^{\ell_{n-1}}y_{n-1}(z)$.

The specific technique of this section is to construct a sequence $s_0, s_1, \ldots$ of shifts that obeys a particular recursion (see Section 4.1), and then use generating functions to express $C_{x_n,y_n}(s_n)$ in terms of the values $C_{x_m,y_m}(s_m)$ and $C_{x_m,y_m}(-s_m)$ for some $m < n$ (see Section 4.2). This provides a bound (see Section 4.3) that will be used in Section 5 to fill in the gap left by the bounds in Section 3 (see the discussion before Notation 3.4).

4.1. A recursion on shifts.

We begin by defining a recursion for a sequence $s_0, s_1, \ldots$ of shifts, and then we explore the properties of sequences obeying this recursion.

Definition 4.1 (Shift Recursion Rule)**.** We say that an infinite sequence of integers $s_0, s_1, \ldots$ follows the *shift recursion rule* to mean that $s_{n+1} = -s_n - \ell_n$ for each $n \in \mathbb{N}$.

Definition 4.2 (Standard Shift Sequence)**.** For each $n \in \mathbb{N}$, define $t_n = ((-1)^n - 2^n)\ell_0/3$. We call the sequence $t_0, t_1, \ldots$ the *standard shift sequence.*

Remark 4.3. Observe that the standard shift sequence $t_0, t_1, \ldots$ follows the shift recursion rule, that is, $t_{n+1} = -t_n - \ell_n$.

Lemma 4.4. *Suppose that $s_0, s_1, \ldots$ follows the shift recursion rule and let $t_0, t_1, \ldots$ be the standard shift sequence. Then $s_n = t_n + (-1)^n s_0$.*

Proof. We induct on $n \in \mathbb{N}$ with the base case being trivial since $t_0 = 0$. Then we suppose that the statement holds for some $n \geq 0$, add ℓ_n to both sides, and negate our equation to get $-s_n - \ell_n = -t_n - \ell_n + (-1)^{n+1}s_0$. Then use the shift recursion rule to see that $s_{n+1} = t_{n+1} + (-1)^{n+1}s_0$. □

Lemma 4.5. *Suppose $s_0, s_1, \ldots$ follows the shift recursion rule. Then there is some $n \in \mathbb{N}$ such that $|s_n| < \ell_n$. Let m be the least nonnegative integer such that $|s_m| < \ell_m$. If $|s_0| < \ell_0$, then $m = 0$. If $s_0 \geq \ell_0$ (resp., $s_0 \leq -\ell_0$) then m is the least even (resp., odd) integer with $m > -2 + \log_2((-1)^m(3s_0+\ell_0)/\ell_0)$.*

Proof. Let $t_0, t_1, \ldots$ be the standard shift sequence. By Lemma 4.4 we have $s_n = t_n + (-1)^n s_0 = ((-1)^n - 2^n)\ell_0/3 + (-1)^n s_0 = (-1)^n(3s_0+\ell_0)/3 - \ell_n/3$, so that

$$-\ell_n < s_n < \ell_n \text{ if and only if } -\frac{2}{3}\ell_n < \frac{(-1)^n(3s_0+\ell_0)}{3} < \frac{4}{3}\ell_n. \tag{9}$$

Since $\lim_{n\to\infty} \ell_n = \lim_{n\to\infty} 2^n \ell_0 = \infty$, there is some $n \in \mathbb{N}$ such that $-\ell_n < s_n < \ell_n$, thus proving existence. So we may indeed define m to be the smallest nonnegative value of n such that the equivalent statements in (9) hold. If $|s_0| < \ell_0$, then it is immediate that $m = 0$ by the definition of m.

Suppose, for a contradiction, that $s_0 \geq \ell_0$ and m is odd, or that $s_0 \leq -\ell_0$ and m is even. Then $-2\ell_{m-1}/3 < 0 < (-1)^{m-1}(3s_0+\ell_0)/3$, and by negating the third inequality in (9) with $n = m$ we have $(-1)^{m-1}(3s_0+\ell_0)/3 < 2\ell_m/3 = 4\ell_{m-1}/3$. Therefore $-2\ell_{m-1}/3 < (-1)^{m-1}(3s_0+\ell_0)/3 < 4\ell_{m-1}/3$, which by (9) contradicts the minimality assumption on m. Thus, m must be even (resp., odd) if $s_0 \geq \ell_0$ (resp., $s_0 \leq -\ell_0$). When $s_0 \geq \ell_0$ (resp., $s_0 \leq -\ell_0$) and n is even (resp., odd), the third inequality in (9) always holds, so m must be the least even (resp., odd) value of n that makes the fourth inequality in (9) hold, i.e., the least even (resp., odd) integer such that $(-1)^m(3s_0+\ell_0)/3 < 2^{m+2}\ell_0/3$. □

Lemma 4.6. *If $s_0, s_1, \ldots$ follows the shift recursion rule, then the following hold.*

(i) If $0 \leq s_n < \ell_n$, then $-\ell_{n+1} < s_{n+1} \leq -\ell_n$.
(ii) If $-\ell_n < s_n < 0$, then $-\ell_n < s_{n+1} < 0$.
(iii) If $s_n \leq -\ell_n$, then $s_{n+1} \geq 0$.
(iv) If $s_n \geq \ell_n$, then $s_{n+1} \leq -\ell_{n+1}$.

Proof. All four statements follow easily from the shift recursion rule. □

Corollary 4.7. *Let $s_0, s_1, \ldots$ follow the shift recursion rule, and let m be the smallest nonnegative integer such that $|s_m| < \ell_m$ (which exists by Lemma 4.5). Then we have the following:*

(i) $0 \leq s_m < \ell_m$ if $m > 0$ or $\ell_0 = 1$,
(ii) $-\ell_n < s_n < 0$ for all $n > m$, and
(iii) For all $n \in \mathbb{N}$ with $n < m$, we have $s_n \geq \ell_n$ if $n \equiv m \pmod 2$ and $s_n \leq -\ell_n$ if $n \not\equiv m \pmod 2$.

Proof. If $m = 0$ and $\ell_0 = 1$, then our assumption that $|s_m| < \ell_m$ forces $s_m = s_0 = 0$, and so $0 \leq s_m < \ell_m$. If $m > 0$, then $s_m > -\ell_m$ by assumption, so the contrapositive of Lemma 4.6(iv) makes $s_{m-1} < \ell_{m-1}$, but we must have $|s_{m-1}| \geq \ell_{m-1}$ by the minimality of m, so that $s_{m-1} \leq -\ell_{m-1}$, which in turn implies $s_m \geq 0$ by Lemma 4.6(iii), and thus our initial assumption that $|s_m| < \ell_m$ implies $0 \leq s_m < \ell_m$. This proves (i).

Now we prove (ii). Once we have an n such that $-\ell_n < s_n < 0$, then $-\ell_{n+1} < -\ell_n < s_{n+1} < 0$ by Lemma 4.6(ii). So if $-\ell_m < s_m < 0$, we are done. Otherwise, $0 \leq s_m < \ell_m$, and then Lemma 4.6(i) shows that $-\ell_{m+1} < s_{m+1} \leq -\ell_m < 0$.

For the last statement, since $|s_n| \geq \ell_n$ for all $n \in \mathbb{N}$ with $n < m$, Lemma 4.6(iii) and (iv) show that $s_0, s_1, \ldots, s_{m-1}$ is a sequence of nonzero integers with alternating signs, and since $s_m > -\ell_m$, its immediate predecessor, s_{m-1}, must be less than or equal to $-\ell_{m-1}$. □

4.2. **A generating function for crosscorrelations.** We now prove some relations on the crosscorrelation of Golay–Rudin–Shapiro sequences evaluated at shifts satisfying the shift recursion rule.

Lemma 4.8. *If $s_0, s_1, \ldots$ follows the shift recursion rule, and $n > 1$ with $s_n < 0$, then*

$$C_{x_n,y_n}(s_n) = -C_{x_{n-1},y_{n-1}}(-s_{n-1}) + 2C_{x_{n-2},y_{n-2}}(s_{n-2}), \text{ and}$$
$$C_{x_n,y_n}(-s_n) = \overline{C_{x_{n-1},y_{n-1}}(-s_{n-1})} + 2\overline{C_{x_{n-2},y_{n-2}}(s_{n-2})}.$$

Proof. Use Lemma 2.11 with $s = s_n < 0$ (resp., $s = -s_n > 0$) and rewrite the shifts using the shift recursion rule to obtain the first (resp., second) relation. □

Proposition 4.9. *If $s_0, s_1, \ldots$ follows the shift recursion rule, $n > 2$, $s_{n-1} < 0$, and $s_n < 0$, then we have*

$$C_{x_n,y_n}(s_n) = \overline{C_{x_{n-1},y_{n-1}}(s_{n-1})} + 2C_{x_{n-2},y_{n-2}}(s_{n-2}) - 4\overline{C_{x_{n-3},y_{n-3}}(s_{n-3})}.$$

Proof. Consider the two relations in Lemma 4.8 when n is replaced by $n-1$; if we add the conjugate of the first to the second and rearrange, we obtain

$$C_{x_{n-1},y_{n-1}}(-s_{n-1}) = -\overline{C_{x_{n-1},y_{n-1}}(s_{n-1})} + 4\overline{C_{x_{n-3},y_{n-3}}(s_{n-3})},$$

and if we write the expression on the right-hand side of this equation in place of the $C_{x_{n-1},y_{n-1}}(-s_{n-1})$ that appears in the first relation of Lemma 4.8, we obtain the desired result. □

Now we use the above relations to obtain a generating function that organizes crosscorrelations of Golay–Rudin–Shapiro sequences at shifts following the shift recursion rule. The generating function involves the algebraic number $\alpha_0 = 1.658967\ldots$, which is the unique real root of $X^3 + X^2 - 2X - 4$, along with the two non-real conjugate roots, α_1 and α_2, all of which are discussed in Section 2.4.

Proposition 4.10. *Let $s_0, s_1, \ldots$ be a sequence of integers following the shift recursion rule, and let m be the least nonnegative integer such that $|s_m| < \ell_m$. Let $\sigma \colon \mathbb{C} \to \mathbb{C}$ denote the complex conjugation automorphism,* *so $\sigma^k(x) = x$ if k is even and $\sigma^k(x) = \overline{x}$ if k is odd. For each $v \in \{0,1\}$ and $k \in \mathbb{N}$, let $f_{v,k} = \sigma^{v+k}(C_{x_k,y_k}((-1)^v s_k))$. Then for every $n \geq m$, we have*

$$f_{0,n} = \sum_{j \in \mathbb{Z}/3\mathbb{Z}} \sum_{v \in \{0,1\}} E_{j,v} f_{v,m} (-\alpha_j)^{n-m},$$

where $E_{j,0} = (2 + \alpha_{j+1}\alpha_{j+2})/((\alpha_j - \alpha_{j+1})(\alpha_j - \alpha_{j+2}))$ and $E_{j,1} = -(1 + \alpha_{j+1} + \alpha_{j+2})/((\alpha_j - \alpha_{j+1})(\alpha_j - \alpha_{j+2}))$ for each $j \in \mathbb{Z}/3\mathbb{Z}$.

Proof. Since $|s_k| \geq \ell_k$ for $k \in \{0, 1, \ldots, m-1\}$, we know that $f_{0,k} = 0$ for $k < m$. Then for all $k \geq m$ we have $f_{0,k+3} - f_{0,k+2} - 2f_{0,k+1} + 4f_{0,k} = 0$ by Proposition 4.9 since s_{k+3} and s_{k+2} are negative by Corollary 4.7(ii). This recursion has characteristic polynomial $X^3 - X^2 - 2X + 4$ with roots $-\alpha_0$, $-\alpha_1$, and $-\alpha_2$. Therefore,

$$f_{0,n} = c_0(-\alpha_0)^n + c_1(-\alpha_1)^n + c_2(-\alpha_2)^n \tag{10}$$

for some constants c_1, c_2 and c_3. So we can solve a linear system to express c_0, c_1, and c_2 in terms of $f_{0,m}$, $f_{0,m+1}$, and $f_{0,m+2}$:

$$c_j = \frac{\alpha_{j+1}\alpha_{j+2} f_{0,m} + (\alpha_{j+1} + \alpha_{j+2}) f_{0,m+1} + f_{0,m+2}}{(-\alpha_j)^m (\alpha_j - \alpha_{j+1})(\alpha_j - \alpha_{j+2})}$$

for each $j \in \mathbb{Z}/3\mathbb{Z}$. Now Lemma 4.8 with $n = m+2$ gives $f_{0,m+2} = -f_{1,m+1} + 2f_{0,m}$ and when $n = m+1$, Lemma 4.8 gives $f_{1,m+1} = f_{1,m}$ (since $f_{0,k} = 0$ when $k < m$) so that $f_{0,m+2} = -f_{1,m} + 2f_{0,m}$. Also, Lemma 4.8 with $n = m+1$ gives $f_{0,m+1} = -f_{1,m}$ so we get

$$c_j = (-\alpha_j)^{-m} \left[\frac{(2 + \alpha_{j+1}\alpha_{j+2}) f_{0,m} - (1 + \alpha_{j+1} + \alpha_{j+2}) f_{1,m}}{(\alpha_j - \alpha_{j+1})(\alpha_j - \alpha_{j+2})} \right]$$

for $j \in \mathbb{Z}/3\mathbb{Z}$. We obtain the final result by substituting these values of c_j into (10). □

4.3. **Bounds from the generating function.** Now we show how to use Proposition 4.10 to obtain bounds on the peak crosscorrelation of Golay–Rudin–Shapiro sequences from bounds for sequences appearing earlier in the recursion. This method almost provides an inductive proof of our bounds in Theorems 1.3–1.5, but it works only for crosscorrelation values at shifts satisfying a particular condition (the $n \geq m + 9$ hypothesis in Proposition 4.11 below), and so the chain of induction cannot always be completed. It is possible to prove results similar to Proposition 4.11 with less stringent conditions, but were not able to find a version that works in full generality. Therefore we deemed it impractical to attempt an inductive proof Theorems 1.3–1.5 based solely this generating function method, but we did find that this method works in the critical cases where the method from Section 3 fails; this enables us to prove our theorems in Section 5.

Proposition 4.11. *Let $s_0, s_1, \ldots$ be a sequence of integers following the shift recursion rule, and let m be the least nonnegative integer such that $|s_m| <$*

ℓ_m. Suppose that $n \geq m+9$ and that K is a positive real number and that $|C_{x_j,y_j}(s)| \leq K\alpha_0^j$ for all $s \in \mathbb{Z}$ and all $0 \leq j < n$. Then $|C_{x_n,y_n}(s_n)| \leq K\alpha_0^n$.

Proof. For each $j \in \mathbb{Z}/3\mathbb{Z}$, $v \in \{0,1\}$, and $k \in \mathbb{N}$, define $E_{j,v}$ and $f_{v,k}$ as in Proposition 4.10. Define $F_{v,g} = \sum_{j \in \mathbb{Z}/3\mathbb{Z}} E_{j,v}(-\alpha_j/\alpha_0)^g$ for each $v \in \{0,1\}$ and $g \in \mathbb{N}$. We change the order of summation in the expression from Proposition 4.10 to obtain

$$f_{0,n} = \sum_{v \in \{0,1\}} f_{v,m} F_{v,n-m} \alpha_0^{n-m}.$$

Divide both sides by $K\alpha_0^n$ and take the absolute value to get

$$\begin{aligned} \frac{|f_{0,n}|}{K\alpha_0^n} &= \left| \sum_{v \in \{0,1\}} \frac{f_{v,m}}{K\alpha_0^m} F_{v,n-m} \right| \\ &\leq \sum_{v \in \{0,1\}} |F_{v,n-m}|, \end{aligned}$$

where the inequality comes from the triangle inequality and the fact that for each $v \in \{0,1\}$, we have $|f_{v,m}|/(K\alpha_0^m) = |C_{x_m,y_m}((-1)^v s_m)|/(K\alpha_0^m)$, which lies in the real interval $[0,1]$ by assumption. Therefore, if we can show $F_{0,n-m} + (-1)^u F_{1,n-m}$ lies in the real interval $[-1,1]$ for each $u \in \{0,1\}$, then we will be done.

Define $G_{j,u} = E_{j,0} + (-1)^u E_{j,1}$ for each $u \in \{0,1\}$ and $j \in \mathbb{Z}/3\mathbb{Z}$. So it suffices to show that $\sum_{j \in \mathbb{Z}/3\mathbb{Z}} G_{j,u}(-\alpha_j/\alpha_0)^{n-m}$ lies in $[-1,1]$, or equivalently, that $\sum_{j \in \mathbb{Z}/3\mathbb{Z}} G_{j,u}(\alpha_j/\alpha_0)^{n-m}$ lies in $[-1,1]$, for each $u \in \{0,1\}$.

Since α_0 is real and α_1 and α_2 are a conjugate pair of non-reals, we see that $E_{0,v}$ is real and $E_{1,v}$ and $E_{2,v}$ are a conjugate pair for each $v \in \{0,1\}$, so that $G_{0,u}$ is real and $G_{1,u}$ and $G_{2,u}$ are a conjugate pair for each $u \in \{0,1\}$. So it suffices to show that $G_{0,u} + 2\operatorname{Re}(\rho^{n-m}G_{1,u})$ lies in $[-1,1]$, where $\rho = \alpha_1/\alpha_0$, or equivalently, it suffices to show that $\operatorname{Re}(\rho^{n-m}G_{1,u})$ lies in $[(-1-G_{0,u})/2, (1-G_{0,u})/2]$ for each $u \in \{0,1\}$.

We may now use the techniques of Section 2.4 to show that $0 < G_{0,u} < 1$ for $u \in \{0,1\}$. Thus it will suffice to show that $\operatorname{Re}(\rho^{n-m}G_{1,u})$ lies in the smaller interval $[(-1+G_{0,u})/2, (1-G_{0,u})/2]$ for each $u \in \{0,1\}$. At the end of Section 2.4, it was noted that $|\alpha_1| < |\alpha_0|$, so $|\rho| < 1$. Since $n - m \geq 9$, it suffices to prove that $|\rho|^9 \leq (1-G_{0,u})/(2|G_{1,u}|)$, which is true if and only if $|\rho|^{18} \leq (1-G_{0,u})^2/(4|G_{1,u}|^2)$, i.e., $\alpha_1^9\alpha_2^9/\alpha_0^{18} \leq (1-G_{0,u})^2/(4G_{1,u}G_{2,u})$, a fact that can be checked for each $u \in \{0,1\}$ using the procedures laid out in Section 2.4. □

5. Bounds from shifts in the recursion

We are now ready to combine the bound from Proposition 3.7 with the bound from Proposition 4.11 into an inductive proof that gives a bound on the peak crosscorrelation of sequence pairs produced by the Golay–Rudin–Shapiro recursion. Then we deduce bounds on the peak sidelobe level from these. In Section 5.1, we show that shifts for which we cannot get a good bound on their crosscorrelation using Proposition 3.7 are shifts for which we can get a good bound with Proposition 4.11. Then in Section 5.2, we prove bounds on correlation for the particular case of the Rudin–Shapiro sequences, and finally in Section 5.3 we prove more general bounds that cover the full range of Golay pairs generated by the Golay–Rudin–Shapiro recursion (Definition 1.1).

Recall that throughout this paper ℓ_n, x_n, y_n are always as in Definition 1.1: ℓ_0 is a positive integer and x_0 and y_0 are nonzero polynomials in $\mathbb{C}[z]$ of degree less than ℓ_0 such that (x_0, y_0) is a Golay complementary pair with $C_{x_0,x_0}(0) = C_{y_0,y_0}(0)$, and for every $n \in \mathbb{N}$, we have $\ell_n = 2^n\ell_0$ and (x_n, y_n) is the nth Golay pair obtained from ℓ_0 and the seed pair (x_0, y_0) via the Golay–Rudin–Shapiro recursion: $x_n(z) = x_{n-1}(z) + z^{\ell_{n-1}}y_{n-1}(z)$ and $y_n(z) = x_{n-1}(z) - z^{\ell_{n-1}}y_{n-1}(z)$.

5.1. **Complementarity of Propositions 3.7 and 4.11.**

We now show that the small range of shifts that the $t = 10$ case of Proposition 3.7 cannot handle can be dealt with using Proposition 4.11.

Lemma 5.1. *Let $n, s \in \mathbb{Z}$ with $n \geq 11$, and let $s_0, s_1, \dots$ be the unique sequence following the shift recursion rule with $s_n = s$. Suppose that $s_n \in (-342\ell_{n-10}, -341\ell_{n-10})$, and let m be the least nonnegative integer such that $|s_m| < \ell_m$. Then $n - m \geq 11$.*

Proof. If $|s_0| < \ell_0$, then $m = 0$ and $n-m = n-0 \geq 11$ by assumption. So let us assume $|s_0| \geq \ell_0$ henceforth. Let $t_0, t_1, \dots$ be the standard shift sequence as in Definition 4.2. Recall from Lemma 4.4 that $(-1)^n s_0 = s_n - t_n$. Since s_n lies in $(-342\ell_{n-10}, -341\ell_{n-10})$ and $t_n = ((-1)^n - 2^n)\ell_0/3$, we have

$$(-1)^n s_0 = s_n - t_n \in \left(\frac{-2 \cdot 2^{n-10}\ell_0 - (-1)^n\ell_0}{3}, \frac{2^{n-10}\ell_0 - (-1)^n\ell_0}{3}\right).$$

In the case where $s_0 \geq \ell_0$, Lemma 4.5 says that m is the least even integer with $m > -2 + \log_2((3s_0 + \ell_0)/\ell_0)$. When n is even (resp., odd), we have $s_0 \in \left[\ell_0, (2^{n-10}\ell_0 - \ell_0)/3\right)$ (resp., $s_0 \in \left[\ell_0, (2^{n-9}\ell_0 - \ell_0)/3\right)$), so then $-2 + \log_2((3s_0 + \ell_0)/\ell_0)$ lies in $[0, n-12)$ (resp., $[0, n-11)$), and since m is the least even integer greater than this, we have $m \leq n-12$ (resp., $m \leq n-11$).

In the case where $s_0 \leq -\ell_0$, Lemma 4.5 says that m is the least odd integer with $m > -2 + \log_2(-(3s_0 + \ell_0)/\ell_0)$. When n is even (resp., odd), we have $s_0 \in \left((-2^{n-9}\ell_0 - \ell_0)/3, -\ell_0\right]$ (resp., $s_0 \in \left((-2^{n-10}\ell_0 - \ell_0)/3, -\ell_0\right]$), so then $-2+\log_2(-(3s_0 + \ell_0)/\ell_0)$ lies in $[-1, n-11)$ (resp., $[-1, n-12)$), and since m is the least odd integer greater than this, we have $m \leq n-11$ (resp., $m \leq n-12$). □

5.2. **Bounds on peak correlation for Rudin–Shapiro sequences.**

Recall the algebraic number $\alpha_0 = 1.658967\dots$, which appears in our bounds in Theorems 1.3–1.5, and whose technical details are described in Section 2.4.

Lemma 5.1 now enables us to use Proposition 3.7 and Proposition 4.11 to prove the upper bounds in Theorems 1.3 and 1.4.

Theorem 5.2. *If $n \in \mathbb{N}$ and x_n and y_n are the nth Rudin–Shapiro sequence and its companion, then* $\mathrm{PCC}(x_n, y_n) \leq 5\alpha_0^{n-3} = (1.095107\ldots)\alpha_0^n$*. This upper bound becomes an equality if $n = 3$; otherwise it is a strict inequality. We also have* $\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n) \leq 5\alpha_0^{n-4} = (0.660113...)\alpha_0^n$*. This upper bound becomes an equality if $n = 4$; otherwise it is a strict inequality.*

Proof. We begin by proving the bound on $\mathrm{PCC}(x_n, y_n)$. We write C_n for $x_n\overline{y_n}$, and then $C_{n,s}$ is the coefficient of z^s in C_n; this coefficient is the same as $C_{x_n,y_n}(s)$. We let $K = 5\alpha_0^{-3}$, and we need to show that $|C_{n,s}| \leq K\alpha_0^n$ for all $n \in \mathbb{N}$ and $s \in \mathbb{Z}$. We proceed by induction on n. We shall prove the $n = 0$ and $n = 1$ cases directly below. When $n \geq 2$, we set $t = n - 1$ and use Proposition 3.7 (noting that $\ell_{n-t} = \ell_1 = 2\ell_0 = 2$ for our Rudin–Shapiro sequences) to establish the bound for most shifts, leaving only some exceptional shifts that need to be checked. When $n > 0$, we also pass over even values of s in silence, since $C_{n,s} = 0$ for those values by Lemma 2.12. In what follows, when we assert an inequality involving powers of α_0, we have verified it using the methods of Section 2.4.

(0) If $n = 0$, then since x_0 and y_0 are of degree 0, we need only consider $s = 0$, for which, using Table 1, we find that $C_{0,0} = 1 \leq 5\alpha_0^{-3} = K\alpha_0^0$.

(1) If $n = 1$, then since x_1 and y_1 are of degree 1, we need only consider $s \in \{-1, 1\}$ for which, using Table 1, we find that $|C_{1,s}| = 1 \leq 5\alpha_0^{-2} = K\alpha_0^1$.

(2) If $n = 2$, then Proposition 3.7 with $t = 1$ shows that we need only consider $s \in \{-1, 1\}$ for which, using Table 1, we find that $|C_{2,s}| \leq 3 \leq 5\alpha_0^{-1} = K\alpha_0^2$.

(3) If $n = 3$, then Proposition 3.7 with $t = 2$ shows that we need only consider $s \in \{-3, 1, 1, 3\}$ for which, using Table 1, we find that $|C_{3,s}| \leq 5 = K\alpha_0^3$.

(4) If $n = 4$, then Proposition 3.7 with $t = 3$ shows that we need only consider $s \in \{-7, -5, 3, 5\}$ for which, using Table 1, we find that $|C_{4,s}| \leq 7 \leq 5\alpha_0 = K\alpha_0^4$.

(5) If $n = 5$, then Proposition 3.7 with $t = 4$ shows that we need only consider $s \in \{-11, 5, 9, 11\}$ for which, using Table 1, we find that $|C_{5,s}| \leq 13 \leq 5\alpha_0^2 = K\alpha_0^5$.

(6) If $n = 6$, then Proposition 3.7 with $t = 5$ shows that we need only consider $s \in \{-23, -21, 11, 19, 21\}$ for which, using Table 1, we find that $|C_{6,s}| \leq 15 \leq 5\alpha_0^3 = K\alpha_0^6$.

(7) If $n = 7$, then Proposition 3.7 with $t = 6$ shows that we need only consider $s \in \{-45, -43, 21, 23, 37, 43\}$ for which, using Table 1, we find that $|C_{7,s}| \leq 33 \leq 5\alpha_0^4 = K\alpha_0^7$.

(8) If $n = 8$, then Proposition 3.7 with $t = 7$ shows that we need only consider $s \in \{-91, -85, 43, 75, 85\}$ for which, using Table 1, we find that $|C_{8,s}| \leq 49 \leq 5\alpha_0^5 = K\alpha_0^8$.

(9) If $n = 9$, then Proposition 3.7 with $t = 8$ shows that we need only consider $s \in \{-181, -171, 85, 149\}$ for which, using Table 1, we find $|C_{9,s}| \leq 83 \leq 5\alpha_0^6 = K\alpha_0^9$.

(10) If $n = 10$, then Proposition 3.7 with $t = 9$ shows that we need only consider $s \in \{-363, -361, -341, 299\}$ for which, using Table 1, we find that $|C_{10,s}| \leq 153 \leq 5\alpha_0^7 = K\alpha_0^{10}$.

(11) Now suppose that $n \geq 11$ and that $|C_{j,s}| \leq K\alpha_0^j$ for all $0 \leq j < n$ and $s \in \mathbb{Z}$. Then Proposition 3.7 with $t = 10$ shows us that we need only consider $s \in (-342\ell_{n-10}, -341\ell_{n-10})$. Define $s_0, s_1, \ldots$ to be the unique sequence following the shift recursion rule with $s_n = s$. Define m to be the least nonnegative integer such that $|s_m| < \ell_m$. Then by Lemma 5.1, $n - m \geq 11 \geq 9$. Therefore Proposition 4.11 shows $|C_{n,s}| \leq K\alpha_0^n$.

Thus, we have proved that $\mathrm{PCC}(x_n, y_n) \leq 5\alpha_0^{n-3}$ for every $n \in \mathbb{N}$. This inequality becomes an equality when $n = 3$, because $|C_{x_3,y_3}(-3)| = |-5| = 5\alpha_0^{3-3}$ (see Table 1). When $n \neq 3$, we know that $5\alpha_0^{n-3}$ is irrational by 2.21, and since $\mathrm{PCC}(x_n, y_n)$ must be an integer (since x_n and y_n are binary sequences), the upper bound must be a strict equality.

Since $x_0 = y_0 = 1$, we have $C_{x_0,x_0}(s) = C_{y_0,y_0}(s) = 0$ for all nonzero s, so $\mathrm{PSL}(x_0) = \mathrm{PSL}(y_0) = 0 < 5\alpha_0^{0-4}$. For $n > 0$ we have $\mathrm{PSL}(y_n) = \mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1}, y_{n-1}) \leq 5\alpha_0^{(n-1)-3}$ (where the inequality becomes an equality if and only if $n - 1 = 3$); the first equality comes from Lemma 2.4, the second equality is from Lemma 2.10, and the inequality is what we just proved. Furthermore, we can show $5\alpha_0^{n-3} = 1.095107\ldots$ and $5\alpha_0^{-4} = 0.660113...$ using the methods of Section 2.4. □

One might wonder if it is possible to devise an exponential bound for $\mathrm{PCC}(x_n, y_n)$ with a lower base than α_0. The following result shows that this is not possible.

Proposition 5.3. *If x_n and y_n the nth Rudin–Shapiro sequence and its companion for each $n \in \mathbb{N}$, and if $t_0, t_1, \ldots$ is the standard shift sequence, then*

$$\left|\frac{C_{x_n,y_n}(t_n)}{(-\alpha_0)^n} - \frac{9\alpha_0^2 + 4\alpha_0 + 6}{59}\right| \leq 2\sqrt{\frac{-4\alpha_0^2 + 2\alpha_0 + 14}{59}} \left(\sqrt{\frac{\alpha_0^2 - 1}{2}}\right)^n,$$

that is,

$$\left|\frac{C_{x_n,y_n}(t_n)}{(-\alpha_0)^n} - 0.633990\ldots\right| \leq (0.654022\ldots)(0.935994\ldots)^n,$$

and so,

$$\frac{\mathrm{PCC}(x_n, y_n)}{\alpha_0^n} \geq \frac{9\alpha_0^2 + 4\alpha_0 + 6}{59} - 2\sqrt{\frac{-4\alpha_0^2 + 2\alpha_0 + 14}{59}} \left(\sqrt{\frac{\alpha_0^2 - 1}{2}}\right)^n$$
$$= (0.633990\ldots) - (0.654022\ldots)(0.935994\ldots)^n.$$

We also have

$$\begin{aligned}\frac{\mathrm{PSL}(x_n)}{\alpha_0^n} &\geq \frac{3\alpha_0^2+21\alpha_0+2}{118} - \sqrt{\frac{6\alpha_0^2+6\alpha_0-16}{59}}\left(\sqrt{\frac{\alpha_0^2-1}{2}}\right)^n \\ &= (0.382159\ldots) - (0.421193\ldots)(0.935994\ldots)^n.\end{aligned}$$

Proof. We first prove the bound involving $C_{x_n,y_n}(t_n)$. Recall that the standard shift sequence $t_0, t_1, \ldots$ follows the shift recursion rule by Remark 4.3, and it has $-\ell_0 < t_0 = 0 < \ell_0$. So we can use $t_0, t_1, \ldots$ as $s_0, s_1, \ldots$ with $m = 0$ in Proposition 4.10, whose notations for σ, $f_{v,k}$ and $E_{j,v}$ we also adopt. Since $t_0 = 0$ and $m = 0$, we have $f_{0,m} = C_{x_0,y_0}(0) = 1$ and $f_{1,m} = \overline{C_{x_0,y_0}(-0)} = 1$. For each $j \in \mathbb{Z}/3\mathbb{Z}$, set $E_j = E_{j,0} + E_{j,1}$. Then, Proposition 4.10 tells us that $\sigma^n(C_{x_n,y_n}(t_n)) = E_0(-\alpha_0)^n + E_1(-\alpha_1)^n + E_2(-\alpha_2)^n$, and since x_n and y_n are the Rudin–Shapiro sequences, we know that $C_{x_n,y_n}(t_n) \in \mathbb{Z}$, so in fact $C_{x_n,y_n}(t_n) = E_0(-\alpha_0)^n + E_1(-\alpha_1)^n + E_2(-\alpha_2)^n$. If we divide both sides by $-\alpha_0^n$, subtract E_0, and take the absolute value (recalling that, we obtain

$$\left|\frac{C_{x_n,y_n}(t_n)}{(-\alpha_0)^n} - E_0\right| = \left|E_1\left(\frac{\alpha_1}{\alpha_0}\right)^n + E_2\left(\frac{\alpha_2}{\alpha_0}\right)^n\right|.$$

Since α_0 is real while α_1 and α_2 are complex conjugates, one can deduce from the definition of $E_{j,v}$ in Proposition 4.10 that $E_{1,v}$ and $E_{2,v}$ are a conjugate pair for each $v \in \{0,1\}$, and so E_1 and E_2 are complex conjugates. Thus

$$\left|\frac{C_{x_n,y_n}(t_n)}{(-\alpha_0)^n} - E_0\right| \leq 2|E_1|\left|\frac{\alpha_1}{\alpha_0}\right|^n. \tag{11}$$

The methods of Section 2.4 show that $E_0 = E_{0,0} + E_{0,1}$ is a positive number equal to $(9\alpha_0^2 + 4\alpha_0 + 6)/59 = 0.633990\ldots$. Since E_1 and E_2 are conjugates, we have $|E_1|^2 = E_1E_2$; the methods of Section 2.4 show this to be equal to $(-4\alpha_0^2 + 2\alpha_0 + 14)/59$, and they also show that $0.654022^2 < 4E_1E_2 < 0.654023^2$, so that $2|E_1| = \sqrt{4E_1E_2} = 0.654022\ldots$. Lemma 2.20 shows that $|\alpha_1/\alpha_0| = \sqrt{(\alpha_0^2-1)/2} = 0.935994\ldots$.

By definition, $\mathrm{PCC}(x_n, y_n) \geq |C_{x_n,y_n}(t_n)|$, so we have

$$\begin{aligned}\frac{\mathrm{PCC}(x_n,y_n)}{\alpha_0^n} &\geq \left|\frac{C_{x_n,y_n}(t_n)}{(-\alpha_0)^n}\right| \\ &\geq E_0 - 2|E_1|\left|\frac{\alpha_1}{\alpha_0}\right|^n,\end{aligned} \tag{12}$$

where the second inequality uses (11), and numerical approximations of the quantities in the last expression have already been discussed above.

We now prove the bound on $\mathrm{PSL}(x_n)$. Suppose that $n > 0$. Then Lemma 2.10 shows that $\mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1}, y_{n-1})$, and we can use the bound we already proved to show that

$$\begin{aligned}\frac{\mathrm{PSL}(x_n)}{\alpha_0^n} &= \frac{1}{\alpha_0}\cdot\frac{\mathrm{PCC}(x_{n-1},y_{n-1})}{\alpha_0^{n-1}}\\ &\geq \frac{1}{\alpha_0}\left(E_0-2|E_1|\left|\frac{\alpha_1}{\alpha_0}\right|^{n-1}\right)\\ &= \frac{E_0}{\alpha_0}-2\left|\frac{E_1}{\alpha_1}\right|\left|\frac{\alpha_1}{\alpha_0}\right|^{n},\end{aligned}$$

where we use (12) to obtain the inequality. We already have an expression for $|\alpha_1/\alpha_0|$. We can use the methods of Section 2.4 to show that E_0/α_0 is a positive number equal to $(3\alpha_0^2+21\alpha_0+2)/118 = 0.382159\ldots$. Since α_0 is positive real, while α_1 and α_2 are complex conjugates, and E_1 and E_2 are complex conjugates, we know that $(2|E_1/\alpha_1|)^2 = 4E_1E_2/(\alpha_1\alpha_2)$; the methods of Section 2.4 show this to be equal to $(6\alpha_0^2+6\alpha_0-16)/59$, and they also show that $0.421193^2 < 4E_1E_2/(\alpha_1\alpha_2) < 0.421194^2$, so that $2|E_1/\alpha_1| = \sqrt{4E_1E_2/(\alpha_1\alpha_2)} = 0.431193\ldots$. This proves the desired bound on $\mathrm{PSL}(x_n)$ for $n > 0$, and the desired bound is trivial for $n = 0$, since it is asserting that $\mathrm{PSL}(x_0)$ is larger than a negative number. □

Remark 5.4. Theorem 5.2 and Proposition 5.3, when taken together, show that $0.633990\ldots \leq \limsup_{n\to\infty}\mathrm{PCC}(x_n,y_n)/\alpha_0^n \leq 1.095107\ldots$ when x_n and y_n are the nth Rudin–Shapiro sequence and its companion. Therefore, our bound in Theorem 5.2 is sharp in the following sense:

- No exponential bound with a base $\beta < \alpha_0$ is possible.
- If the bound is to hold for all $n \in \mathbb{N}$, we cannot lower the constant prefactor $1.095107\ldots$ since when $n = 3$, the upper bound is met.

Similarly, we have $0.382159\ldots \leq \limsup_{n\to\infty}\mathrm{PSL}(x_n)/\alpha_0^n \leq 0.660113\ldots$, and our bound on $\mathrm{PSL}(x_n)$ (and on $\mathrm{PSL}(y_n)$ since $\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n)$ by Lemma 2.4) is sharp in the same sense as the bound for $\mathrm{PCC}(x_n,y_n)$ is.

Proposition 5.3 gives a lower bound on $\mathrm{PCC}(x_n,y_n)$ which is not very strong when n is small (indeed, it is negative when $n = 0$). We can use our computer calculations of $\mathrm{PCC}(x_n,y_n)$ for small n to prove a lower bound that is much better for small n, although for large n the bound in Proposition 5.3 is better.

Proposition 5.5. *If x_n and y_n are the nth Rudin–Shapiro sequence and its companion for each $n \in \mathbb{N}$, then we have $\mathrm{PCC}(x_n,y_n) \geq 133991557\alpha_0^{n-38} = (0.593256\ldots)\alpha_0^n$, where the $\geq$ becomes an equality when $n = 38$, but is a strict inequality otherwise. This lower bound on $\mathrm{PCC}(x_n,y_n)$ is strictly stronger than that of Proposition 5.3 for $n \leq 41$, but strictly weaker for $n \geq 42$. For $n \geq 1$, we have $\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n) \geq 133991557\alpha_0^{n-39} = (0.357605\ldots)\alpha_0^n$, where the $\geq$ becomes an equality when $n = 39$, but is a strict inequality otherwise. This lower bound on $\mathrm{PSL}(x_n)$ is strictly stronger than that of Proposition 5.3 for $n \leq 42$, but strictly weaker for $n \geq 43$.*

Proof. Let $A = (9\alpha_0^2 + 4\alpha_0 + 6)/59$, $B = 4(-4\alpha_0^2 + 2\alpha_0 + 14)/59$, and $C = (\alpha_0^2 - 1)/2$, so that the lower bound in Proposition 5.3 says that $\mathrm{PCC}(x_n, y_n) \geq (A - \sqrt{BC^n})\alpha_0^n$. Let $D = 133991557/\alpha_0^{38}$, which the methods of Section 2.4 show to be $0.593256\ldots$; the lower bound we wish to prove here is $\mathrm{PCC}(x_n, y_n) \geq D\alpha_0^n$. Showing that this bound is strictly stronger (resp., weaker) than the bound of Proposition 5.3 for a given n is equivalent to showing that $A - D$ is less (resp., greater) than $\sqrt{BC^n}$, and since $A - D$ is positive (as can be verified using the methods of Section 2.4), this is equivalent to showing that $(A - D)^2$ is less (resp., greater) than BC^n. We know from Proposition 5.3 that $C < 1$ (since $\sqrt{C} = 0.935994\ldots$), and the methods of Section 2.4 can be used to show that $(A - D)^2 < BC^{41}$ but $(A - D)^2 > BC^{42}$, thus verifying the claim about the strength of the bound of Proposition 5.3 relative to the bound $\mathrm{PCC}(x_n, y_n) \leq D\alpha_0^n$, which we wish to prove. Thus we only need to prove the latter bound for $n \leq 41$, and from the values of $\mathrm{PCC}(x_n, y_n)$ we obtain by perusing Table 3, we use the methods of Section 2.4 to check that $\mathrm{PCC}(x_n, y_n) \leq 133991557\alpha_0^{n-38}$ is indeed true for all such n. When $n = 38$, the value of $\mathrm{PCC}(x_n, y_n)$ from Table 3 shows that this upper bound becomes an equality. When $n \neq 38$, we know that $133991557\alpha_0^{n-38}$ is irrational by 2.21, and since $\mathrm{PCC}(x_n, y_n)$ must be an integer (since x_n and y_n are binary sequences), the lower bound must be a strict inequality.

For every $n > 0$ we have $\mathrm{PSL}(y_n) = \mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1}, y_{n-1}) \geq 133991557\alpha_0^{(n-1)-38}$ (where the inequality becomes an equality if and only if $n - 1 = 38$); the first equality comes from Lemma 2.4, the second equality is from Lemma 2.10, and the inequality is what we just proved. The claim about the strength of this lower bound on $\mathrm{PSL}(x_n)$ relative to that of Proposition 5.3 follows if one notes that both of these lower bounds are just the lower bounds for $\mathrm{PCC}(x_{n-1}, y_{n-1})$ from here and from Proposition 5.3, and we know that former is stronger for $n-1 \leq 41$ and the latter is stronger for $n - 1 \geq 42$. The methods of Section 2.4 show that $133991557/\alpha_0^{39}$ is $0.357605\ldots$. □

5.3. **General bounds.** In the previous section, we focused specifically on Rudin–Shapiro sequences, but in this section, we consider Golay–Rudin–Shapiro sequences produced by Definition 1.1 in its full generality. For this more general class of sequences, we obtain the correlation bounds given in Theorem 1.5, which we restate here. These general bounds are written in terms of the peak correlation values for the seed pair (x_0, y_0), i.e., $\mathrm{PCC}(x_0, y_0)$ and $\mathrm{PSL}(x_0)$.

Theorem 5.6. *Suppose that ℓ_n, x_n, and y_n are as in Definition 1.1, and that $K = 9\alpha_0^{-4}\,\mathrm{PCC}(x_0, y_0) + 18\alpha_0^{-5}\,\mathrm{PSL}(x_0)$. Then $\mathrm{PCC}(x_n, y_n) \leq K\alpha_0^n$ for every $n \in \mathbb{N}$ and $\mathrm{PSL}(x_n) = \mathrm{PSL}(y_n) \leq K\alpha_0^{n-1}$ for every $n > 0$.*

Proof. We begin by proving the bound on $\mathrm{PCC}(x_n, y_n)$. We write C_n for $x_n\overline{y_n}$ and then $C_{n,s}$ is the coefficient of z^s in C_n; this coefficient is the same as $C_{x_n,y_n}(s)$. We let $L = \mathrm{PCC}(x_0, y_0)$ and $L' = \mathrm{PSL}(x_0)$. We proceed by induction on n. We shall prove the $n = 0$ and $n = 1$ cases directly below. When $n \geq 2$, we set $t = n-1$ and use Proposition 3.7 to establish the bound for most shifts, leaving only some exceptional shifts that need to be checked. For $2 \leq n \leq 10$, we check exceptional shift values s using Lemma 3.6 with $q = \lfloor s/\ell_2 \rfloor$. In what follows, when we assert an inequality involving powers of α_0, we have verified it using the methods of Section 2.4.

(0) If $n = 0$, then $|C_{0,s}| \leq L \leq 9\alpha_0^{-4}L + 18\alpha_0^{-5}L' = K\alpha_0^0$, where the first inequality follows from the definition of L, and the second follows from $1 \leq 9\alpha_0^{-4}$.

(1) If $n = 1$, then $|C_{1,s}| \leq L + 2L' \leq 9\alpha_0^{-3}L + 18\alpha_0^{-4}L' = K\alpha_0^1$, where the first inequality follows by Lemma 2.14, and the second follows from $1 \leq 9\alpha_0^{-3}$ and $2 \leq 18\alpha_0^{-4}$.

(2) If $n = 2$, then Proposition 3.7 with $t = 1$ shows that we need only consider $s \in (-\ell_1, \ell_1)$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-1, 0\}$. Then we have $|C_{2,s}| \leq 3L + 1 \cdot 2L' \leq 9\alpha_0^{-2}L + 18\alpha_0^{-3}L' = K\alpha_0^2$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 1$, and the second follows from $3 \leq 9\alpha_0^{-2}$ and $2 \leq 18\alpha_0^{-3}$.

(3) If $n = 3$, then Proposition 3.7 with $t = 2$ shows that we need only consider $s \in (-2, 2) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-1, 0\}$. Then we have $|C_{3,s}| \leq 5L + 3 \cdot 2L' \leq 9\alpha_0^{-1}L + 18\alpha_0^{-2}L' = K\alpha_0^3$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 2$, and the second follows from $5 \leq 9\alpha_0^{-1}$ and $6 \leq 18\alpha_0^{-2}$.

(4) If $n = 4$, then Proposition 3.7 with $t = 3$ shows that we need only consider $s \in ((-4, -2) \cup (1, 3)) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-2, 0, 1\}$. Then we have $|C_{4,s}| \leq \max\{7L+5\cdot 2L', 9L+3\cdot 2L'\} \leq 9L+18\alpha_0^{-1}L' = K\alpha_0^4$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 3$, and the second follows from $10 \leq 18\alpha_0^{-1}$.

(5) If $n = 5$, then Proposition 3.7 with $t = 4$ shows that we need only consider $s \in ([-6, -5) \cup (2, 3) \cup [4, 6)) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-3, 1, 2\}$. Then we have $|C_{5,s}| \leq \max\{13L + 3 \cdot 2L', 11L + 9 \cdot 2L'\} \leq 9\alpha_0 L + 18L' = K\alpha_0^5$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 4$, and the second follows from $13 \leq 9\alpha_0$.

(6) If $n = 6$, then Proposition 3.7 with $t = 5$ shows that we need only consider $s \in ([-12, -10) \cup (5, 6) \cup (9, 11)) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-6, 2, 4, 5\}$. Then we have $|C_{6,s}| \leq \max\{15L + 13 \cdot 2L', 21L + 7 \cdot 2L', 17L+11\cdot 2L'\} \leq 9\alpha_0^2 L+18\alpha_0 L' = K\alpha_0^6$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 5$, and the second follows from $21 \leq 9\alpha_0^2$ and $26 \leq 18\alpha_0$.

(7) If $n = 7$, then Proposition 3.7 with $t = 6$ shows that we need only consider $s \in \big((-23, -21) \cup (10, 12) \cup (18, 19) \cup (21, 22)\big) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-12, -11, 5, 9, 10\}$. Then we have $|C_{7,s}| \leq \max\{35L+ 9\cdot 2L', 27L+21\cdot 2L', 33L+15\cdot 2L', 31L+17\cdot 2L'\} \leq 9\alpha_0^3 L+18\alpha_0^2 L' = K\alpha_0^7$, where the first inequality follows by Lemma 3.6 using Table 2

with $t = 6$, and the second inequality follows from $35 \leq 9\alpha_0^3$ and $42 \leq 18\alpha_0^2$.

(8) If $n = 8$, then Proposition 3.7 with $t = 7$ shows that we need only consider $s \in \big((-46,-45) \cup (-43,-42) \cup (21,22) \cup (37,38) \cup (42,43)\big) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-23,-22,10,18,21\}$. Then we have $|C_{8,s}| \leq \max\{47L+33\cdot 2L', 49L+31\cdot 2L', 51L+21\cdot 2L'\} \leq 9\alpha_0^4 L + 18\alpha_0^3 L' = K\alpha_0^8$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 7$, and the second follows from $51 \leq 9\alpha_0^4$ and $66 \leq 18\alpha_0^3$.

(9) If $n = 9$, then Proposition 3.7 with $t = 8$ shows that we need only consider $s \in \big((-91,-90) \cup (-86,-85) \cup (42,43) \cup (74,75)\big) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-46,-43,21,37\}$. Then we have $|C_{9,s}| \leq \max\{99L + 33\cdot 2L', 91L + 49\cdot 2L'\} \leq 9\alpha_0^5 L + 18\alpha_0^4 L' = K\alpha_0^9$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 8$, and the second follows from $99 \leq 9\alpha_0^5$ and $98 \leq 18\alpha_0^4$.

(10) If $n = 10$, then Proposition 3.7 with $t = 9$ shows that we need only consider $s \in ((-182,-180) \cup (-171,-170) \cup (149,150)) \cdot \ell_1$, so that $q = \lfloor s/\ell_2 \rfloor \in \{-91,-86,74\}$. Then we have $|C_{10,s}| \leq \max\{109L + 99\cdot 2L', 153L + 55\cdot 2L', 117L + 87\cdot 2L'\} \leq 9\alpha_0^6 L + 18\alpha_0^5 L' = K\alpha_0^{10}$, where the first inequality follows by Lemma 3.6 using Table 2 with $t = 9$, and the second follows from $153 \leq 9\alpha_0^6$ and $198 \leq 18\alpha_0^5$.

(11) Now suppose that $n \geq 11$ and that $|C_{j,s}| \leq K\alpha_0^j$ for all $0 \leq j < n$ and $s \in \mathbb{Z}$. Then Proposition 3.7 with $t = 10$ shows that we need only consider $s \in (-342\ell_{n-10}, -341\ell_{n-10})$. Define $s_0, s_1, \ldots$ to be the unique sequence following the shift recursion rule that has $s_n = s$. Define m to be the least nonnegative integer such that $|s_m| < \ell_m$. Then by Lemma 5.1, $n - m \geq 11 \geq 9$. Therefore, Proposition 4.11 shows that $|C_{n,s}| \leq K\alpha_0^n$.

Thus, we have proved that $\mathrm{PCC}(x_n, y_n) \leq K\alpha_0^n$ for every $n \in \mathbb{N}$. For $n > 0$ we have $\mathrm{PSL}(y_n) = \mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1}, y_{n-1}) \leq K\alpha_0^{n-1}$, where the first equality comes from Lemma 2.4, the second is from Lemma 2.10, and the inequality is what we just proved. □

One might wonder if it is possible to devise an exponential bound for $\mathrm{PCC}(x_n, y_n)$ with a lower base than α_0. The following result shows that this is not possible.

Proposition 5.7. *Let ℓ_n, x_n, and y_n be as in Definition 1.1, and let $\sigma\colon \mathbb{C} \to \mathbb{C}$ be the complex conjugation automorphism. Then there is some sequence $s_0, s_1, \ldots$ of integers following the shift recursion rule with $|s_0| < \ell_0$ such that*

$$M = \frac{(\alpha_0^2 + 7\alpha_0 + 40)C_{x_0,y_0}(s_0) + (17\alpha_0^2 + \alpha_0 - 28)\overline{C_{x_0,y_0}(-s_0)}}{118}$$

is nonzero, and if we set

$$N = |C_{x_0,y_0}(s_0)|\sqrt{\frac{-4\alpha_0+24}{59}} + |C_{x_0,y_0}(-s_0)|\sqrt{\frac{-2\alpha_0^2+10\alpha_0+12}{59}},$$

then

$$\begin{aligned}\left|\frac{\sigma^n(C_{x_n,y_n}(s_n))}{(-\alpha_0)^n} - M\right| &\leq N\left(\sqrt{\frac{\alpha_0^2-1}{2}}\right)^n \\ &= N(0.935994\ldots)^n,\end{aligned}$$

and so

$$\begin{aligned}\frac{\mathrm{PCC}(x_n,y_n)}{\alpha_0^n} &\geq |M| - N\left(\sqrt{\frac{\alpha_0^2-1}{2}}\right)^n \\ &= |M| - N(0.935994\ldots)^n.\end{aligned}$$

Proof. Since α_0 is a real number and $\{1,\alpha_0,\alpha_0^2\}$ is a $\mathbb{Q}$-linearly independent set, it is clear that $-(17\alpha_0^2+\alpha_0-28)/(\alpha_0^2+7\alpha_0+40)$ is a real number not equal to 1 or -1. We use Lemma 2.16 to obtain some s_0 with $|s_0| < \ell_0$ such that $(\alpha_0^2+7\alpha_0+40)C_{x_0,y_0}(s_0) + (17\alpha_0^2+\alpha_0-28)\overline{C_{x_0,y_0}(-s_0)} \neq 0$, i.e., $M \neq 0$. Then choose $s_1, s_2 \ldots$ so that $s_0, s_1, s_2, \ldots$ follows the shift recursion rule. Define $f_{v,k}$ and $E_{j,v}$ as in Proposition 4.10, and one can use the methods of Section 2.4 to compute that $E_{0,0} = (\alpha_0^2+7\alpha_0+40)/118$ and $E_{0,1} = (17\alpha_0^2+\alpha_0-28)/118$, so that $M = E_{0,0}f_{0,0} + E_{0,1}f_{1,0}$. Then note that $m = 0$ in Proposition 4.10 (because $|s_0| < \ell_0$) so we obtain $f_{0,n} = \sum_{j\in\mathbb{Z}/3\mathbb{Z}}\sum_{v\in\{0,1\}}(-\alpha_j)^n E_{j,v}f_{v,0}$, which we can rearrange and apply the definition of $f_{v,k}$ to obtain

$$\frac{\sigma^n(C_{x_n,y_n}(s_n))}{(-\alpha_0)^n} - M = \sum_{j\in\{1,2\}}\sum_{v\in\{0,1\}} E_{j,v}\sigma^v(C_{x_0,y_0}((-1)^v s_0))\left(\frac{\alpha_j}{\alpha_0}\right)^n.$$

If we take the absolute value of both sides, apply the triangle inequality, remember that α_1 and α_2 are complex conjugates, and recognize that $E_{1,v}$ and $E_{2,v}$ is a conjugate pair for each $v \in \{0,1\}$ (see the definitions in Proposition 4.10), we obtain

$$\left|\frac{\sigma^n(C_{x_n,y_n}(s_n))}{(-\alpha_0)^n} - M\right| \leq \left|\frac{\alpha_1}{\alpha_0}\right|^n \sum_{v\in\{0,1\}} 2|E_{1,v}||C_{x_0,y_0}((-1)^v s_0)|.$$

Then we use the methods of Section 2.4 to see that $4|E_{1,0}|^2 = 4E_{1,0}E_{2,0} = (-4\alpha_0+24)/59$ and $4|E_{1,1}|^2 = 4E_{1,1}E_{2,1} = (-2\alpha_0^2+10\alpha_0+12)/59$, so that we recognize the sum over v on the right-hand side as N, while Lemma 2.20 shows that $|\alpha_1/\alpha_0| = \sqrt{(\alpha_0^2-1)/2} = 0.935994\ldots$. This completes the proof of the first bound, and the second bound follows immediately since $\mathrm{PCC}(x_n,y_n)$ upper bounds all crosscorrelation values for x_n with y_n. □

Remark 5.8. Theorem 5.6 and Proposition 5.7, when taken together, show that $\limsup_{n\to\infty} \mathrm{PCC}(x_n,y_n)/\alpha_0^n$ is a strictly positive real number. Therefore, no exponential bound on $\mathrm{PCC}(x_n,y_n)$ with a base $b<\alpha_0$ is possible. Furthermore, by Lemma 2.4 and Lemma 2.10, which say that $\mathrm{PSL}(y_n) = \mathrm{PSL}(x_n) = \mathrm{PCC}(x_{n-1},y_{n-1})$ for $n \geq 1$, we know that our bounds on $\mathrm{PSL}(x_n)$ and $\mathrm{PSL}(y_n)$ are also sharp in the same sense.

Acknowledgement

The authors thank an anonymous reviewer for suggestions that helped improve the paper.

References

[ACD$^+$19] J.-P. Allouche, S. Choi, A. Denise, T. Erdélyi, and B. Saffari. Bounds on autocorrelation coefficients of Rudin-Shapiro polynomials. *Anal. Math.*, 45(4):705–726, 2019.

[BL01] Peter Borwein and Richard Lockhart. The expected L_p norm of random polynomials. *Proc. Amer. Math. Soc.*, 129(5):1463–1472, 2001.

[BM00] Peter Borwein and Michael Mossinghoff. Rudin-Shapiro-like polynomials in L_4. *Math. Comp.*, 69(231):1157–1166, 2000.

[Cho20] Stephen Choi. Bounds on autocorrelation coefficients of Rudin-Shapiro polynomials II. *J. Approx. Theory*, 254:105390, 26, 2020.

[GG05] Solomon W. Golomb and Guang Gong. *Signal design for good correlation.* Cambridge University Press, Cambridge, 2005.

[Gol51] Marcel J. E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Am.*, 41(7):468–472, 1951.

[Gol61] Marcel J. E. Golay. Complementary series. *IRE Trans.*, IT-7:82–87, 1961.

[Gol67] Solomon W. Golomb. *Shift register sequences.* With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam, 1967.

[Gol72] Marcel J. E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, 18:449–450, 1972.

[Gol75] Marcel J. E. Golay. Hybrid low autocorrelation sequences. *IEEE Trans. Inform. Theory*, 21:460–462, 1975.

[HJJ85] Tom Høholdt, Helge Elbrønd Jensen, and Jørn Justesen. Aperiodic correlations and the merit factor of a class of binary sequences. *IEEE Trans. Inform. Theory*, 31(4):549–552, 1985.

[Kat16] Daniel J. Katz. Aperiodic crosscorrelation of sequences derived from characters. *IEEE Trans. Inform. Theory*, 62(9):5237–5259, 2016.

[KLT20a] Daniel J. Katz, Sangman Lee, and Stanislav A. Trunov. Crosscorrelation of Rudin-Shapiro-like polynomials. *Appl. Comput. Harmon. Anal.*, 48(2):513–538, 2020.

[KLT20b] Daniel J. Katz, Sangman Lee, and Stanislav A. Trunov. Rudin-Shapiro-like sequences with maximum asymptotic merit factor. *IEEE Trans. Inform. Theory*, 66(12):7728–7738, 2020.

[KM21] Daniel J Katz and Eli Moore. Sequence pairs with lowest combined autocorrelation and crosscorrelation. arXiv:1711.02229 [cs.IT], 2021.

[Lit68] John E. Littlewood. *Some problems in real and complex analysis.* D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.

[Rud59] Walter Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959.

[Sar84] D. V. Sarwate. Mean-square correlation of shift-register sequences. *Communications, Radar and Signal Processing, IEE Proceedings F*, 131(2):101–106, April 1984.

[Sch09] M. R. Schroeder. *Number theory in science and communication.* Springer-Verlag, Berlin, fifth edition, 2009.

[Sha51] Harold S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, Massachusetts Institute of Technology, Cambridge, 1951.

[Tag96] M. Taghavi. An estimate on the correlation coefficients of the Rudin-Shapiro polynomials. *Iranian J. Sci. Tech.*, 20(2, Trans. A Sci.):235–240, 1996.

[Tag97] M. Taghavi. Upper bounds for the autocorrelation coefficients of the Rudin-Shapiro polynomials. *Korean J. Comput. Appl. Math.*, 4(1):39–46, 1997.

[Tag07] M. Taghavi. Autocorrelation for a class of polynomials with coefficients defined on T. *Iran. J. Sci. Technol. Trans. A Sci.*, 31(4):391–396, 2007.

Department of Mathematics, California State University, Northridge, United States