Constructions of Boolean Correctors with Optimal Nonlinearity and Vectorial Correctors Beyond Optimal Linear Correction Order

Zhaole Li, and Deng Tang

Abstract

Correctors are postprocessing functions that reduce or eliminate statistical bias in raw bitstreams produced by physical noise sources in true random number generators. In this paper, we develop a framework based on binary Krawtchouk polynomials for analyzing and constructing Boolean and vectorial correctors. This framework reformulates the Walsh-layer criterion into finite moment constraints on support-layer counts and preimage-layer counts. We also establish universal upper bounds on the nonlinearity of correctors, and necessary conditions on the achievable correction order. For Boolean functions, we prove that $(n-1)$-correctors are either the parity function or its complement. Then we characterize the support-layer profiles of $(n-2)$- and $(n-3)$-correctors and establish upper bounds on nonlinearity. For $n = 2^k \geq 8$, a self-addressing construction yields $(n-2)$-correctors achieving the optimal nonlinearity $2^{n-1} - 2^{n-1}/n$ with resiliency $n/2 - 2$ and algebraic degree $k+1$. Notably, this provides the first known infinite family of nonlinear correctors achieving both optimal correction order and optimal nonlinearity for that order, while having a resiliency strictly lower than the correction order. Furthermore, using constant-weight addressing, we construct $(n-d-1)$-correctors that asymptotically meet the nonlinearity upper bounds for every fixed $d \geq 1$. Our profile characterization also reveals inherent limitations of injective Maiorana–McFarland constructions at correction order $n-3$. For vectorial functions, we construct nonlinear $(s(2^m-1), m, s2^{m-1}+\ell-1)$-correctors for every $m \geq 2$ under certain conditions on s and ℓ, with resiliency at most $s2^{m-1}-2$. To the best of our knowledge, this is the first infinite family of nonlinear correctors whose correction order simultaneously exceeds that of optimal linear corrector and its own resiliency. Finally, we introduce a secondary construction that lifts these vectorial correctors to larger input dimensions while preserving their correction-order advantage. This approach yields a nonlinearity of $2^{n-1} - 2^{n-n_0-1}$, where n_0 is the input dimension of the base corrector, along with explicit resiliency and a flexible algebraic degree.

Index Terms

Boolean function, Corrector, Nonlinearity, Resiliency, Walsh spectrum, True random number generator

I. Introduction

RANDOM number generators (RNGs) are crucial to the security of cryptographic systems. Typical applications include key generation, initialization vectors, and countermeasures against side-channel attacks. Two kinds of generators exist, pseudorandom and true random number generators (PRNGs and TRNGs, respectively). PRNGs are usually faster and their outputs have better statistical properties, but the numbers generated are predictable. TRNGs, by contrast, derive randomness from physical phenomena such as circuit noise, phase jitter, and metastability [1, 2, 3]. Their outputs are intrinsically unpredictable, but the underlying physical sources can be slow and can exhibit bias or statistical dependence. To mask imperfections of the output and correct the biased random sequences, an effective postprocessor is required.

Under TRNG standards such as NIST SP 800-90B [4], ISO/IEC 20543 [5], and AIS 31 [6], postprocessing methods are commonly divided into cryptographic and algorithmic procedures. Cryptographic postprocessing employs primitives like hash functions or block ciphers in CMAC mode [4] to obtain computational indistinguishability. However, it suffers from high hardware area, latency [7], and intractable analytical bias bounds. The classical study of algorithmic postprocessing dates back to von Neumann [8], who showed that independent unbiased bits can be extracted from a nondegenerate independent identically distributed (i.i.d.) Bernoulli source with unknown bias. Hoeffding and Simons [9] subsequently investigated more efficient sequential procedures, while Dwass [10] extended the problem to nondegenerate i.i.d. discrete random variables, aiming to generate uniformly distributed outputs over a finite alphabet. Subsequently, along this line, more algorithms for generating unbiased bits tossing from a biased coin were proposed [11, 12, 13, 14, 15, 16]. The essential problem is an unbounded worst-case waiting time until the next output bit becomes available, which is an unsatisfactory situation for one who has to use the random numbers.

In contrast, fixed-block postprocessing maps a fixed number of input bits to a fixed number of output bits and aims to suppress the remaining statistical bias. Probably the simplest method is XOR [17] a fixed n input bits to get one output bit. Dichtl [18] investigated this under the case of **independent input bits with a constant bias** e and proposed transformations

(Corresponding author: Deng Tang.)

The authors are with the School of Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: z.l.li@foxmail.com; dtang@foxmail.com).

0000–0000 © 2023 IEEE

that eliminate low-order terms in the output-bias polynomials. Building on this fixed-block approach, Lacharme [19] expressed output bias under the same assumption as a polynomial in the common input-bias parameter e, with coefficients determined by the Walsh spectrum. The valuation of a nonzero bias polynomial is the degree of its lowest-degree nonzero term, where higher valuation implies stronger bias correction. The following year, Lacharme [20] formalized c-correctors by requiring valuation at least $c+1$. For vectorial functions, this condition applies to every nonzero linear combination of the output coordinates. He pointed out that every c-resilient function is a c-corrector, but the converse fails. He also showed that an $[n, m, d]$ linear code can give an n-input m-output linear corrector with a correction order of $d-1$. However, such correctors have identical correction order and resiliency. Subsequent work has begun to separate the two parameters. Recently, Zhang [21] was the first to consider the construction of nonlinear correctors whose correction order exceeds their resiliency. He used a pair of disjoint equidistant linear codes to construct correctors with high nonlinearity and algebraic degree, achieving a correction order that exceeds the resiliency order by 1. He also raised the open question of finding a general construction method for a c-corrector that is not c-resilient. More recently, Walsh spectral neutralization and resilient fragmentary method have been used to construct n-variable semi-bent correctors [22, 23], respectively, providing an improved trade-off between nonlinearity and correction order. The $(n-2)$-correctors with higher nonlinearity compared to [21] are also constructed in [22]. Notably, Grenouilloux et al. [24] used binary Krawtchouk polynomials to characterize the correction order of Boolean functions, and then derived the resiliency of weightwise almost perfectly balanced functions. However, two main problems remain. First, the best nonlinearity of (n, m, c)-correctors is unknown. Second, no constructions of nonlinear (n, m, c)-correctors with correction order simultaneously exceeding that of the optimal linear corrector and its own resiliency are known.

In this paper, we study those problems using binary Krawtchouk polynomials, which converts Lacharme's spectral criterion [20] into finite moment constraints on support counts and the preimage sizes across Hamming layers. We give equivalent spectral and combinatorial criteria for Boolean correctors, and extend this description to vectorial correctors. We also derive universal upper bounds on nonlinearity and establish necessary conditions for the existence of (n, m, c)-correctors. In the Boolean case, we first show that correction order $n-1$ permits only parity and its complement. Then, we characterize the layer profiles of $(n-2)$- and $(n-3)$-correctors and derive upper bounds on their nonlinearity. For every $n = 2^k \geq 8$, a self-addressing construction achieves the proved upper bound on nonlinearity for $(n-2)$-correctors, with $\mathrm{NL}(f) = 2^{n-1} - 2^{n-1}/n$, resiliency $n/2-2$ and algebraic degree $k+1$. To the best of our knowledge, this provides the first infinite family of $(n-2)$-correctors with optimal nonlinearity, while admitting a resiliency less than the correction order. For each fixed $d \geq 1$, constant-weight address constructions yield families of correction order $n-d-1$ asymptotically meeting the upper bound on nonlinearity. By the characterization of $(n-3)$-correctors, we also establish the limitation for injective MM $(n-3)$-correctors. In the vectorial case, we construct nonlinear $(s(2^m-1), m, s2^{m-1}+\ell-1)$-correctors for every $m \geq 2$, with s, ℓ satisfying certain conditions. These constructions have correction order $s2^{m-1}+\ell-1$, which exceeds the optimal linear correction order $s2^{m-1}-1$ in the same parameter regime, while their resiliency is at most $s2^{m-1}-2$. To the best of our knowledge, this is the first infinite family of nonlinear (n, m, c)-correctors whose correction order is strictly larger than that of the optimal linear corrector and its own resiliency. We further develop a secondary construction to lift these correctors to $((2^m-1)(L+s), m, 2^{m-1}(L+s)+\ell-1)$-correctors, where L, s, ℓ satisfy certain conditions. The resulting correctors have best-known nonlinearity $2^{n-1} - 2^{n-n_0-1}$, resiliency $2^{m-1}L-1$ and flexible algebraic degree, where $n_0 = s(2^m-1)$ is the input dimension of the original corrector.

The remainder of the paper is organized as follows. Section II fixes the notation and recalls the Walsh, resiliency, and corrector criteria. Section III develops Krawtchouk inversion and layer profiles. Section IV establishes upper bounds on nonlinearity and necessary conditions for the existence of (n, m, c)-correctors. Section V investigates higher-correction-order Boolean correctors, including the $(n-2)$- and $(n-3)$-correctors, and Section VI develops constructions of vectorial correctors, whose correction orders strictly exceed the optimal linear correction order. Section VII concludes the paper and Appendix provides supplemental proofs, data, and files.

II. Preliminaries

In this section, we introduce the necessary notation, basic definitions, and several lemmas related to Boolean functions and correctors.

A. Notation and Boolean functions

Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field of two elements, and let $\mathbb{F}_2^n$ denote the n-dimensional vector space over $\mathbb{F}_2$. We use the symbol $\oplus$ and $\bigoplus$ to denote the addition over $\mathbb{F}_2$, and $+$ and $\sum$ to denote the integer sum. For simplicity, we also write $+$ in place of $\oplus$ whenever the context is clear. We use $|S|$ to denote the cardinality of the set S. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, their inner product is $x \cdot y = \sum_{i=1}^n x_i y_i$. The Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, denoted by $\mathrm{wt}(x)$, is the number of 1s in x, i.e., $|\{1 \leq i \leq n : x_i = 1\}|$. The Hamming distance between two vectors u and v is defined as $d_H(u, v) = \mathrm{wt}(u \oplus v)$. We use $\mathbf{1}_n$ to denote the all-one vector $(1, \ldots, 1)$ in $\mathbb{F}_2^n$.

An n-variable Boolean function is defined as a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. A function $f \in \mathcal{B}_n$ can be specified by its truth table, which is a vector $(a_0, \ldots, a_{2^n-1}) \in \mathbb{F}_2^{2^n}$ listing the outputs of f in lexicographical order of the inputs. The Hamming weight of $f \in \mathcal{B}_n$ is defined as the cardinality of its support, i.e.,

$\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : f(x) = 1\}|$. Furthermore, any function $f \in \mathcal{B}_n$ has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called its algebraic normal form (ANF),

$$f(x) = \bigoplus_{I \subseteq \{1,\ldots,n\}} \lambda_I \prod_{i \in I} x_i, \quad \lambda_I \in \mathbb{F}_2.$$

Its algebraic degree, denoted by $\deg(f)$, is the maximal value of $|I|$ such that $\lambda_I = 1$. We call a Boolean function with $\deg(f) \leq 1$ affine and the set of all n-variable affine functions is denoted by $\mathcal{A}_n$. An affine function with the constant term equal to zero is called a linear function. A Boolean function $f \in \mathcal{B}_n$ is said to be nonlinear if f is not affine.

B. Walsh transform and resiliency

Definition 1 ([25]). *The Walsh transform of $f \in \mathcal{B}_n$ at point u is a function from $\mathbb{F}_2^n$ to $\mathbb{Z}$, defined by*

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}.$$

The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is the minimum Hamming distance between f and all functions in $\mathcal{A}_n$, i.e.,

$$\mathrm{NL}(f) = \min_{l \in \mathcal{A}_n} d_H(f, l).$$

In terms of Walsh transform, the nonlinearity of f is given by

$$\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2} M(f),$$

where $M(f) = \max_u |W_f(u)|$ is called the maximum Walsh magnitude.

Definition 2 ([26]). *A function $f \in \mathcal{B}_n$ is t-correlation-immune if and only if for each choice of indices $x_{i_1}, \ldots, x_{i_t}$ with $1 \leq i_1 < \cdots < i_t \leq n$,*

$$\Pr(f = c, x_{i_1} = a_1, \ldots, x_{i_t} = a_t) = \frac{1}{2^t} \Pr(f = c),$$

where $(a_1, \ldots, a_t) \in \mathbb{F}_2^t$ and $c \in \mathbb{F}_2$.

The function $f \in \mathcal{B}_n$ is defined as t-resilient, or $\mathrm{res}(f) = t$, if it is balanced and t-correlation-immune. By definition, f is t-resilient if and only if when t inputs of f are fixed to any vector in $\mathbb{F}_2^t$ and the remaining $n - t$ inputs run through all 2^{n-t} input tuples, the output of f remains balanced. Xiao–Massey theorem [27] gives a spectral characterization of resilient functions.

Lemma 1 ([27]). *A function $f \in \mathcal{B}_n$ is t-resilient if and only if its Walsh transform satisfies $W_f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$ such that $0 \leq \mathrm{wt}(\alpha) \leq t$.*

C. Bias and correction order

Let X_i with $i = 1, 2, \ldots, n$, be independent and have a constant bias e, i.e.,

$$\Pr(X_i = a) = \frac{1}{2} + (-1)^a e, \qquad i = 1, 2, \ldots, n, \quad a = 0, 1.$$

If a Boolean function $f \in \mathcal{B}_n$ is used to correct this biased sequence, the output bias $\Delta_f(e)$ of f is given by

$$\Delta_f(e) = \frac{1}{2} \left(\Pr(f(X) = 0) - \Pr(f(X) = 1) \right).$$

Lacharme [19, Theorem 2] gave a polynomial expression for the bias of f from the perspective of Walsh transform of Boolean functions, that is,

$$\Delta_f(e) = \frac{1}{2^{n+1}} \sum_{w \in \mathbb{F}_2^n} (2e)^{\mathrm{wt}(w)} W_f(w).$$

Let $P(X) = \sum_{i=0}^{d} a_i X^i$ be a polynomial of degree d, and the smallest integer $i > 0$ such that $a_i \neq 0$ is called the valuation of $P(X)$. The valuation of $\Delta_f(e)$ is a crucial criterion for measuring the ability of f to reduce output bias.

Definition 3 ([20]). *A balanced Boolean function $f \in \mathcal{B}_n$ is called a c-corrector if the bias $\Delta_f(e)$ is a polynomial with valuation not less than $c + 1$. The integer c is called the correction order of f.*

In the rest of the paper, we say a function is an exact (n, m, c)-correction if it has correction order c.

Lemma 2 ([20]). *$f \in \mathcal{B}_n$ is a c-corrector if and only if for any $0 \le c' \le c$,*

$$\sum_{\substack{u\in\mathbb{F}_2^n \\ \mathrm{wt}(u)=c'}} W_f(u) = 0.$$

It then follows from Xiao-Massey Theorem that a t-resilient Boolean function must be a t-corrector, but the converse is not true in general, see the example after Theorem 7 in [20].

For $0 \le j \le n$, define the Walsh layer sums and their generating polynomial by

$$A_j(f) = \sum_{\mathrm{wt}(u)=j} W_f(u), \qquad P_f(z) = \sum_{j=0}^{n} A_j(f) z^j.$$

By Lemma 2, Lacharme's criterion can be rewritten as

$$f \text{ is a } c\text{-corrector} \iff A_0(f) = \cdots = A_c(f) = 0.$$

D. Vectorial Boolean functions

An (n, m)-function can be viewed as a collection of m Boolean functions $F = (F_1, \ldots, F_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$, where F_i is called a coordinate function of F. The component function of F is defined as the nonzero linear combination of coordinate functions, $F_\lambda = \lambda \cdot F = \sum_{i=1}^m \lambda_i F_i$, where $\lambda \in \mathbb{F}_2^m \setminus \{0\}$. The algebraic degree of F, denoted by $\deg(F)$, is defined as the maximum among the algebraic degrees of all component functions, i.e.,

$$\deg(F) = \max_{\lambda\in\mathbb{F}_2^m\setminus\{0\}} \deg(\lambda \cdot F).$$

The nonlinearity of an (n, m)-function F, denoted by $\mathrm{NL}(F)$, is defined as the minimum of the nonlinearity of all component functions, i.e.,

$$\mathrm{NL}(F) = \min_{\lambda\in\mathbb{F}_2^m\setminus\{0\}} \mathrm{NL}(\lambda \cdot F) = 2^{n-1} - \frac{1}{2} M(F), \qquad M(F) = \max_{u\in\mathbb{F}_2^n,\, \lambda\in\mathbb{F}_2^m\setminus\{0\}} |W_{\lambda\cdot F}(u)|.$$

Lemma 3 ([28]). *An (n, m)-function F is (n, m, t)-resilient if and only if for every nonzero vector $\lambda \in \mathbb{F}_2^m$, $\lambda \cdot F$ is t-resilient, i.e., $\mathrm{res}(F) = \min_{\lambda\neq 0} \mathrm{res}(\lambda \cdot F)$.*

Lemma 4 ([20]). *An (n, m)-function F is an (n, m, c)-corrector if and only if for every nonzero vector $\lambda \in \mathbb{F}_2^m$, $\lambda \cdot F$ is a c-corrector.*

Note that we can construct linear (n, m, c)-correctors by binary linear codes with $c \le c_{\max}^{\mathrm{lin}}(n, m) = d_2(n, m) - 1$, where $d_2(n, m)$ denotes the maximum integer d such that there exists a binary $[n, m, d]$ linear code.

III. Krawtchouk transform and layer profiles

Grenouilloux et al. [24] characterized Boolean correctors through Krawtchouk transforms of restricted Walsh transform and a Vandermonde matrix, and applied this characterization to the resiliency of weightwise almost perfectly balanced functions. In this section, we state its equivalent layer-support-count and inverse-transform formulas, and extends them naturally to the vectorial Boolean function.

For $0 \le w \le n$, let $L_w^{(n)} = \{x \in \mathbb{F}_2^n : \mathrm{wt}(x) = w\}$ denote the w-th Hamming layer. Recall the binary Krawtchouk polynomial $K_j^{(n)}(w)$ is defined by $[z^j](1 + z)^{n-w}(1 - z)^w$, that is, the coefficient of z^j in $(1 + z)^{n-w}(1 - z)^w$,

$$K_j^{(n)}(w) = \sum_{i=0}^{j} (-1)^i \binom{w}{i}\binom{n-w}{j-i}, \qquad \sum_{j=0}^{n} K_j^{(n)}(w) z^j = (1+z)^{n-w}(1-z)^w. \tag{1}$$

We omit the superscripts (n) when the dimension is clear. In this definition, $K_0^{(n)}(w) = 1, K_j^{(n)}(0) = \binom{n}{j}$, and the orthogonality relation [29, 30] yields

$$\sum_{w=0}^{n} \binom{n}{w} K_i^{(n)}(w) K_j^{(n)}(w) = 2^n \binom{n}{j} \mathbf{1}_{\{i=j\}}, \qquad \sum_{w=0}^{n} K_w^{(n)}(i) K_j^{(n)}(w) = 2^n \mathbf{1}_{\{i=j\}}. \tag{2}$$

Indeed, the above two orthogonality relations come from the following reciprocity identity [29], which is a classical property of Krawtchouk polynomials,

$$\binom{n}{w} K_j^{(n)}(w) = \binom{n}{j} K_w^{(n)}(j). \tag{3}$$

For a Boolean function $f \in \mathcal{B}_n$, define its layer support counts and signed layer sums via

$$B_w(f) = |\{x \in L_w : f(x) = 1\}|, \qquad S_w(f) = \binom{n}{w} - 2B_w(f),$$

respectively. Note that our $S_w(f)$ is $\mathcal{W}_{f,w}$ in [24, Definition 5], and Condition (iii) of our Theorem 1 is equivalent to Theorems 1 and 3 of [24]. Then the following theorem reformulates the corrector criterion of [20] in Krawtchouk basis.

Theorem 1 ([24]). *For every Boolean function $f \in \mathcal{B}_n$,*

$$\begin{aligned} A_j(f) &= \sum_{w=0}^{n} S_w(f) K_j(w), && 0 \le j \le n, \\ S_w(f) &= 2^{-n}\binom{n}{w} \sum_{j=0}^{n} \frac{A_j(f)}{\binom{n}{j}} K_j(w) = 2^{-n} \sum_{j=0}^{n} A_j(f) K_w(j), && 0 \le w \le n. \end{aligned} \tag{4}$$

Furthermore, for $0 \le c \le n-1$, the following statements are equivalent,

(i) f is c-corrector,
(ii) For all $0 \le j \le c$, we have $A_j(f) = 0$,
(iii) [24, Theorems 1 and 3] For all $0 \le j \le c$, we have

$$\sum_{w=0}^{n} S_w(f) K_j(w) = 0. \tag{5}$$

(iv) The layer support counts satisfy

$$\sum_{w=0}^{n} B_w(f) = 2^{n-1}, \quad \sum_{w=0}^{n} B_w(f) K_j^{(n)}(w) = 0, \quad 1 \le j \le c. \tag{6}$$

Proof. Interchanging two finite sums gives

$$A_j(f) = \sum_{\mathrm{wt}(u)=j} W_f(u) = \sum_x (-1)^{f(x)} \sum_{\mathrm{wt}(u)=j} (-1)^{u \cdot x} = \sum_w S_w K_j(w).$$

Applying orthogonality relation (2) proves Eq. (4). We only give the proof of (iii) $\iff$ (iv): At $j = 0$, the equation is $\sum_w B_w = 2^{n-1}$. For $j \ge 1$, orthogonality relation (2) with $K_0 = 1$ gives $\sum_w \binom{n}{w} K_j(w) = 0$. Thus Eq. (5) becomes $A_j(f) = -2\sum_w B_w(f) K_j(w)$, proving Eq. (6). □

Consequently, the layer polynomial $P_f(z)$ is completely determined by the layer profile $(B_0(f), \ldots, B_n(f))$. Once this profile is fixed, the support points may be chosen arbitrarily within each Hamming layer.

Corollary 1. *Let $0 \le c \le n-1$, and let $b = (b_0, b_1, \ldots, b_n)$ be an integer vector satisfying*

$$\begin{aligned} &0 \le b_w \le \binom{n}{w}, && 0 \le w \le n, \\ &\sum_{w=0}^{n} b_w = 2^{n-1}, && \sum_{w=0}^{n} b_w K_j^{(n)}(w) = 0, \qquad 1 \le j \le c. \end{aligned}$$

For each w, choose an arbitrary subset $T_w \subseteq L_w^{(n)}$ with $|T_w| = b_w$, and define a Boolean function f_T by $\mathrm{supp}(f_T) = \bigcup_{w=0}^{n} T_w$. Then every such f_T is a c-corrector, and the number of functions generated by this vector is precisely $|\mathcal{C}(b)| = \prod_{w=0}^{n} \binom{\binom{n}{w}}{b_w}$. Its correction order is exactly c if and only if $\sum_w b_w K_{c+1}^{(n)}(w) \neq 0$. Conversely, every c-corrector belongs to a unique support family $\mathcal{C}(b)$.

Proof. Given integers b_w satisfying Condition (iv) in Theorem 1, choose $T_w \subseteq L_w$ of size b_w, the corresponding f_T with $B_w(f_T) = b_w$ satisfying Eq. (6). Since the subsets T_w can be selected independently, yielding $\prod_{w=0}^{n} \binom{\binom{n}{w}}{b_w}$ distinct functions. Finally, by $A_{c+1}(f_T) = -2\sum_{w=0}^{n} b_w K_{c+1}^{(n)}(w)$, the correction order of f_T is strictly greater than c if and only if this sum vanishes. □

Corollary 1 separates the existence of an admissible profile from the choice of support points. All functions in a profile have the same correction order, whereas their Walsh coefficients, nonlinearity, and other cryptographic parameters may differ.

Proposition 1. *Let $f \in \mathcal{B}_n$ be symmetric and $0 \le c \le n-1$, then f is a c-corrector if and only if it is c-resilient.*

Proof. By symmetry, $W_f(u)$ depends only on $j = \mathrm{wt}(u)$, consequently, $A_j(f) = \binom{n}{j} W_f(u_j)$ where $\mathrm{wt}(u_j) = j$, so $A_j(f) = 0$ is equivalent to $W_f(u_j) = 0$ for all $\mathrm{wt}(u_j) = j$. □

This degeneracy demonstrates that constructions achieving high correction order with low resiliency order must exploit asymmetric inner-layer cancellations.

We now extend the characterization of Condition (iv) in Theorem 1 to vectorial Boolean functions. For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $b \in \mathbb{F}_2^m$, let $N_{w,b}(F) = |\{x \in L_w^{(n)} : F(x) = b\}|$ for $0 \le w \le n$. These nonnegative integers illustrate the weight distribution of the preimage $F^{-1}(b)$. Since the preimages $\{F^{-1}(b)\}_{b\in\mathbb{F}_2^m}$ partition each input layer L_w, we have

$$\sum_{b\in\mathbb{F}_2^m} N_{w,b}(F) = \binom{n}{w}, \qquad 0 \le w \le n. \tag{7}$$

Corollary 2. *A function F is an (n, m, c)-corrector if and only if*

$$\sum_{w=0}^{n} N_{w,b} = 2^{n-m}, \qquad \sum_{w=0}^{n} N_{w,b} K_j^{(n)}(w) = 0, \qquad b \in \mathbb{F}_2^m, \qquad 1 \le j \le c. \tag{8}$$

Proof. Define $T_j(b) = \sum_w N_{w,b} K_j(w)$ as a real function on $\mathbb{F}_2^m$, then its Fourier transform over λ yields $\widehat{T_j}(\lambda) = \sum_{b\in\mathbb{F}_2^m} (-1)^{\lambda\cdot b} T_j(b) = A_j(F_\lambda)$. All nontrivial character coefficients vanish if and only if T_j is constant in b. Sum over b determines the constants, that is, $\sum_b T_0(b) = \sum_{w,b} N_{w,b} = 2^n$ implies $T_0(b) = 2^{n-m}$, and $\sum_b T_j(b) = \sum_{w,b} N_{w,b} K_j(w) = \sum_w \binom{n}{w} K_j(w) = 0$ for $j \ge 1$ implies $T_j(b) = 0$. □

IV. Universal bounds on (n, m, c)-correctors

Throughout this section, we assume $n \ge 3, 1 \le m \le n$, $0 \le c \le n-1$, and $Q = 2^{n-m}$. We first combine the layer-profile constraints from Section III with Walsh inversion and orthogonality to establish a joint spectral feasibility bound. We then derive universal upper bounds on nonlinearity and establish Krawtchouk-based necessary conditions for the existence of (n, m, c)-correctors, yielding explicit restrictions on correction order.

A. Universal upper bounds on nonlinearity

For $M \in 4\mathbb{Z}_{\ge 0}$, define the local output spectral set by

$$\mathcal{L}_{m,Q}(M) = \Big\{ \boldsymbol{w} = (w_\lambda)_{\lambda\neq 0} \in (4\mathbb{Z})^{2^m-1} : |w_\lambda| \le M, \\ 2^{-m} \sum_{\lambda\neq 0} (-1)^{\lambda\cdot b} w_\lambda \in \{-Q, -Q+2, \ldots, Q\}, \quad b \in \mathbb{F}_2^m \Big\}. \tag{9}$$

For a nonzero input frequency u, the vector $(W_{F_\lambda}(u))_{\lambda\neq 0}$ belongs to this set when $M = M(F)$. Thus, the set encodes both the range and the parity of these preimage sums, as well as the 4-divisibility of the Walsh coefficients.

We preserve weights $1, \ldots, c$ individually and merge even and odd weights larger than c into E and O, respectively. That is,

$$\mathcal{J}_{n,c} = \{1, \ldots, c, E, O\}, \quad h_j = \binom{n}{j}, \quad h_E = \sum_{\substack{j>c \\ j \text{ even}}} \binom{n}{j}, \quad h_O = \sum_{\substack{j>c \\ j \text{ odd}}} \binom{n}{j},$$

where zero-weight case is omitted. Let $\epsilon_j = j \pmod 2$, $\epsilon_E = 0$, and $\epsilon_O = 1$. For $\delta \in \mathbb{F}_2^m$, let $\mathcal{Z}_{n,m,c}^{\delta}(M)$ denote the set of nonnegative integer arrays $(z_{J,\boldsymbol{w}})_{J\in\mathcal{J}_{n,c}, \boldsymbol{w}\in\mathcal{L}_{m,Q}(M)}$, satisfying

$$\begin{aligned} \sum_{\boldsymbol{w}} z_{J,\boldsymbol{w}} &= h_J, \qquad J \in \mathcal{J}_{n,c}, \\ \sum_{\boldsymbol{w}} z_{j,\boldsymbol{w}} \boldsymbol{w} &= \mathbf{0}_{2^m-1}, \qquad 1 \le j \le c, \\ \sum_{J,\boldsymbol{w}} z_{J,\boldsymbol{w}} \boldsymbol{w} &= 2^n \mathbf{1}_{2^m-1}, \\ \sum_{J,\boldsymbol{w}} (-1)^{\epsilon_J} z_{J,\boldsymbol{w}} \boldsymbol{w} &= 2^n ((-1)^{\lambda\cdot\delta})_{\lambda\neq 0}, \\ \sum_{J,\boldsymbol{w}} z_{J,\boldsymbol{w}} \boldsymbol{w}\boldsymbol{w}^T &= 2^{2n} I_{2^m-1}. \end{aligned} \tag{10}$$

We then define

$$\mathcal{M}_{n,m,c} = \min\big\{ M \in 4\mathbb{Z}_{\ge 0} : \mathcal{Z}_{n,m,c}^{\delta}(M) \neq \emptyset \text{ for some } \delta \in \mathbb{F}_2^m \big\},$$

with the convention $\mathcal{M}_{n,m,c} = +\infty$ if no such M exists.

Theorem 2. *Every (n, m, c)-corrector F satisfies*

$$M(F) \geq \mathcal{M}_{n,m,c}, \quad \mathrm{NL}(F) \leq 2^{n-1} - \frac{1}{2}\mathcal{M}_{n,m,c}. \tag{11}$$

Proof. Normalize $F(0) = 0$ and set $\delta = F(\mathbf{1}_n)$, without changing correction order and nonlinearity. For nonzero u, set $\boldsymbol{w}(u) = (W_{F_\lambda}(u))_{\lambda \neq 0}$, inversion gives

$$2^{-m} \sum_{\lambda \neq 0} (-1)^{\lambda \cdot b} W_{F_\lambda}(u) = \sum_{x : F(x) = b} (-1)^{u \cdot x} \in \{-Q, -Q+2, \ldots, Q\}.$$

Together with four-divisibility, this ensures that $\boldsymbol{w}(u) \in \mathcal{L}_{m,Q}(M(F))$.

Let $z_{J,\boldsymbol{w}}$ count the number of nonzero inputs u in weight class $J \in \mathcal{J}_{n,c}$ such that $\boldsymbol{w}(u) = \boldsymbol{w}$. The first two constraints in Eq. (10) follow from counting and the corrector criterion in Corollary 2. Walsh inversion at 0 and $\mathbf{1}_n$ yields the next two, respectively. The final constraint in Eq. (10) follows from the Gram equality, i.e.,

$$\sum_u W_{F_\lambda}(u) W_{F_\mu}(u) = 2^n \sum_x (-1)^{(\lambda+\mu)\cdot F(x)} = 2^{2n} \mathbf{1}_{\{\lambda = \mu\}}. \qquad \square$$

For a fixed M, the vectors $\boldsymbol{w} \in \mathcal{L}_{m,Q}(M)$ in Eq. (10) are known constants, so these constraints form a finite integer linear feasibility problem in $z_{J,\boldsymbol{w}}$. This formulation serves as a combinatorial relaxation that simultaneously couples the correction order c, the output dimension m, and local spectral integrality. However, this feasibility problem is difficult to solve directly, we therefore derive explicit closed-form relaxations.

For $i = 0, 1$, define the tail weight counts

$$D^{(i)}_{n,c} = \sum_{\substack{j > c \\ j \equiv i \pmod 2}} \binom{n}{j}. \tag{12}$$

Corollary 3. *Let F be an (n, m, c)-corrector with $F(0) = 0$ and $\delta = F(\mathbf{1}_n)$. Define $\Lambda_i = \{\lambda \in \mathbb{F}_2^m \setminus \{0\} : \lambda \cdot \delta = i\}$ for $i = 0, 1$. If $\Lambda_i \neq \emptyset$, then $D^{(i)}_{n,c} > 0$, and*

$$M(F) \geq \max\left\{ 4 \left\lceil \frac{2^{n-2}}{D^{(i)}_{n,c}} \right\rceil,\ 4\left(\left\lfloor 2^{n/2-2} \right\rfloor + 1 \right) \right\}, \qquad |\Lambda_i| \leq D^{(i)}_{n,c}. \tag{13}$$

Proof. Fix $\lambda \in \mathbb{F}_2^m \setminus \{0\}$, and set $h = \lambda \cdot F$, $\sigma_0 = (-1)^{h(0)}$, and $\sigma_1 = (-1)^{h(\mathbf{1}_n)}$. By inverse Walsh transform, $(-1)^{h(x)} = 2^{-n} \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot x} W_h(u)$ for all $x \in \mathbb{F}_2^n$. Evaluating this identity at $x = 0$ and $x = \mathbf{1}_n$ and grouping u by Hamming weight $\mathrm{wt}(u) = j$ yields $\sum_{j=0}^n A_j(h) = 2^n \sigma_0$ and $\sum_{j=0}^n (-1)^j A_j(h) = 2^n \sigma_1$. Since h is a c-corrector, $A_j(h) = 0$ for all $0 \leq j \leq c$. Taking half the sum and half the difference of the two equations above therefore isolates the even and odd tail layers:

$$\sum_{\substack{j > c \\ j \text{ even}}} A_j(h) = 2^{n-1}(\sigma_0 + \sigma_1), \qquad \sum_{\substack{j > c \\ j \text{ odd}}} A_j(h) = 2^{n-1}(\sigma_0 - \sigma_1). \tag{14}$$

Now suppose that $\Lambda_i \neq \emptyset$ and choose $\lambda \in \Lambda_i$. By definition, $h(0) + h(\mathbf{1}_n) = \lambda \cdot (F(0) + F(\mathbf{1}_n)) = \lambda \cdot \delta = i$, so $\sigma_0 \sigma_1 = (-1)^i$. Substituting it into Eq. (14) shows that the sum over the weights $j > c$ with $j \equiv i \pmod 2$ equals $2^n \sigma_0$, whereas the sum over the opposite parity vanishes. Define the index set

$$U_i = \{u \in \mathbb{F}_2^n \setminus \{0\} : \mathrm{wt}(u) > c,\ \mathrm{wt}(u) \equiv i \pmod 2\}, \qquad i = 0, 1,$$

which has cardinality $|U_i| = D^{(i)}_{n,c}$. Expanding $A_j(h)$ in terms of individual Walsh coefficients gives

$$\sum_{u \in U_i} W_{F_\lambda}(u) = 2^n \sigma_0. \tag{15}$$

Since the right-hand side of Eq. (15) is $\pm 2^n \neq 0$, the index set U_i must be nonempty, and hence $D^{(i)}_{n,c} > 0$. To establish the first lower bound on $M(F)$ in Eq. (13), apply the triangle inequality to Eq. (15):

$$2^n = \left| \sum_{u \in U_i} W_{F_\lambda}(u) \right| \leq \sum_{u \in U_i} |W_{F_\lambda}(u)| \leq |U_i| M(F) = D^{(i)}_{n,c} M(F),$$

which implies $M(F)/4 \geq 2^{n-2}/D^{(i)}_{n,c}$. Since $M(F) \in 4\mathbb{Z}_{\geq 0}$, the ratio $M(F)/4$ is an integer, and thus $M(F) \geq 4 \left\lceil 2^{n-2}/D^{(i)}_{n,c} \right\rceil$. For the second term, applying Parseval's identity over the $2^n - 1$ nonzero frequencies and using four-divisibility give $M(F) \geq 4\left(\left\lfloor 2^{n/2-2} \right\rfloor + 1 \right)$.

Next, to bound $|\Lambda_i|$, associate to each $\lambda \in \mathbb{F}_2^m \setminus \{0\}$ the normalized spectral vector $v_\lambda = 2^{-n}(W_{F_\lambda}(u))_{u \neq 0} \in \mathbb{R}^{2^n - 1}$. The Gram identity in the proof of Theorem 2 shows that $\{v_\lambda\}_{\lambda \in \mathbb{F}_2^m \setminus \{0\}}$ forms an orthonormal family in $\mathbb{R}^{2^n-1}$. Let $e_i \in \mathbb{R}^{2^n-1}$

denote the indicator vector of the subset U_i, so that $\|e_i\|^2 = |U_i| = D^{(i)}_{n,c}$. By Eq. (15), for every $\lambda \in \Lambda_i$ we have $\langle e_i, v_\lambda\rangle = 2^{-n}\sum_{u\in U_i} W_{F_\lambda}(u) = \sigma_0 \in \{\pm 1\}$, and hence $|\langle e_i, v_\lambda\rangle|^2 = 1$. Therefore every component in Λ_i has squared projection 1 onto the same vector e_i. Applying Bessel's inequality to the orthonormal subset $\{v_\lambda\}_{\lambda\in\Lambda_i}$ yields

$$\sum_{\lambda\in\Lambda_i} |\langle e_i, v_\lambda\rangle|^2 \le \|e_i\|^2 = D^{(i)}_{n,c},$$

where the left side is $|\Lambda_i|$. □

The above proof implies $2^m - 1 \le D^{(0)}_{n,c} + D^{(1)}_{n,c} = \sum_{r=0}^{n-c-1}\binom{n}{r}$, as Λ_0, Λ_1 partition $\mathbb{F}_2^m \setminus \{0\}$. However, this correction-order-bound is usually weaker than the following Theorem 3.

B. Correction order upper bounds of (n, m, c)-correctors

Even without imposing nonlinearity constraints, Corollary 2 already restricts the admissible parameters (n, m, c). Let $X_n \sim \mathrm{Bin}(n, 1/2)$, Krawtchouk orthogonality gives $\mathbb{E}[K^{(n)}_j(X_n)] = \mathbf{1}_{\{j=0\}}$. Since $K_0, \ldots, K_c$ form a basis for the space of real polynomials of degree at most c, Corollary 2 implies that every polynomial $P \in \mathbb{R}[x]$ of degree at most c satisfies

$$\sum_{w=0}^{n} N_{w,b} P(w) = 2^{n-m}\mathbb{E}[P(X_n)], \qquad b \in \mathbb{F}_2^m. \tag{16}$$

Because the unique input of weight 0 has the image $F(0)$, we have $N_{0,F(0)}(F) = 1$. Evaluating Eq. (16) at $b = F(0)$ for polynomials P that are nonnegative on $0 \le w \le n$ therefore yields $2^{n-m}\mathbb{E}[P(X_n)] \ge P(0)$. Then it is sufficient to find a low-degree polynomial that has the minimal expectation, and is as large as possible at 0, which is classical Christoffel-function problem [29] at 0.

Theorem 3. *Existence of an (n, m, c)-corrector implies*

$$2^{n-m} \ge H_{n,c} := \begin{cases} \displaystyle\sum_{j=0}^{t}\binom{n}{j}, & c = 2t, \\ \displaystyle 2\sum_{j=0}^{t}\binom{n-1}{j}, & c = 2t+1. \end{cases}$$

More generally, define

$$\rho_{n,c} = \max\left\{P(0) : P(x) \ge 0 \text{ for } 0 \le x \le n,\ \mathbb{E}[P(X_n)] = 1,\ \text{degree of } P \text{ is at most } c\right\}. \tag{17}$$

Then $2^{n-m} \ge \rho_{n,c} \ge H_{n,c}$.

Proof. Suppose first $c = 2t$, and take $P = R^2$ of degree at most $2t$ and $R(0) = 1$. Nonnegativity of every summand and $w = 0$ term equals 1 in Eq. (16) gives $1 \le 2^{n-m}\mathbb{E}[R(X_n)^2]$, i.e., $2^{n-m} \ge 1/\mathbb{E}[R(X_n)^2]$. To compute the smallest possible expectation, write $R(w) = \sum_{j=0}^{t} a_j K^{(n)}_j(w)$, then $R(0) = 1$ and orthogonality give, respectively,

$$1 = \sum_{j=0}^{t} a_j\binom{n}{j}, \qquad \mathbb{E}[R(X_n)^2] = \sum_{j=0}^{t} a_j^2\binom{n}{j}.$$

Cauchy–Schwarz implies $\mathbb{E}[R(X_n)^2] \ge \left(\sum_{j=0}^{t}\binom{n}{j}\right)^{-1}$, where equality is achieved when all a_j are equal to $\left(\sum_{k=0}^{t}\binom{n}{k}\right)^{-1}$, hence $2^{n-m} \ge \sum_{j=0}^{t}\binom{n}{j}$.

For $c = 2t+1$, use $P(w) = (1 - w/n)R(w)^2$. It has the right degree $2t+1$, nonnegative at all $0 \le w \le n$, and equals 1 at $w = 0$. The binomial identity $2^{-n}\binom{n}{w}\frac{n-w}{n} = \frac{1}{2}\cdot 2^{-(n-1)}\binom{n-1}{w}$ gives

$$\mathbb{E}[P(X_n)] = \sum_{w=0}^{n} 2^{-n}\binom{n}{w}\left(1 - \frac{w}{n}\right)R(w)^2 = \sum_{w=0}^{n}\frac{1}{2}\cdot 2^{-(n-1)}\binom{n-1}{w}R(w)^2 = \frac{1}{2}\mathbb{E}\left[R(X_{n-1})^2\right].$$

Applying the previous minimization in dimension $n-1$ proves the odd case.

For any feasible function P in Eq. (17), $2^{n-m} = \sum_w N_{w,F(0)}P(w) \ge P(0)$, and taking the maximum over feasible functions yields $2^{n-m} \ge \rho_{n,c}$, the normalized square-polynomial constructed has value $H_{n,c}$ at 0, hence $\rho_{n,c} \ge H_{n,c}$. □

Theorem 3 has an advantage that one can construct

$$P(w) = 1 + \sum_{j=1}^{c}\alpha_j\frac{K^{(n)}_j(w)}{\binom{n}{j}},$$

which automatically gives $\mathbb{E}[P(X_n)] = 1$. The resulting optimization is just a linear program,

$$\begin{aligned} \text{maximize} \quad & 1 + \sum_{j=1}^{c} \alpha_j, \\ \text{subject to} \quad & 1 + \sum_{j=1}^{c} \alpha_j \frac{K_j^{(n)}(w)}{\binom{n}{j}} \geq 0, \quad w \in \{0, \ldots, n\}. \end{aligned}$$

It only has c real variables and $n+1$ nonnegative linear constraints with rational coefficients. It can rule out parameters before a spectral search, especially when m is small.

Corollary 4. *Every $(n, 2, c)$-corrector with $n \geq 4$ satisfies $c \leq n - 3$.*

Proof. For $n = 2k \geq 4$, we obtain $H_{n,n-2} = 2^{n-1} - \frac{1}{2}\binom{2k}{k} > 2^{n-2}$. For $n = 2k+1 \geq 5$, it gives $H_{n,n-2} = 2^{n-1} - \binom{2k}{k} > 2^{n-2}$, where $\binom{2k}{k} < 2^{2k-1}$ for $k \geq 2$. But Theorem 3 with $m = 2$ implies $2^{n-2} \geq H_{n,n-2}$, a contradiction. Thus, there exists no $(n, 2, n-2)$-corrector with $n \geq 4$. □

Suzuki and Iwata [31, Theorems 1 and 2] proves that (n, m, c)-correctors with $m = n, n-1$ have $c = 0, 1$, respectively. By Theorem 3, $H_{n,2} = n + 1 \leq 2^{n-m}$ yields the following broader bound.

Corollary 5. *Every (n, m, c)-corrector with $n + 1 > 2^{n-m}$ satisfies $c \leq 1$.*

The following corollary shows that the Chor et al. [32]'s resiliency bounds $t \leq n - m$ on (n, m, t)-resilient functions also hold for all (n, m, c)-correctors.

Corollary 6. *Every (n, m, c)-corrector satisfies $c \leq n - m$. Furthermore, if $m, c \geq 2$, then $c \leq n - m - 1$.*

Proof. For $c = 2t$, then $n \geq 2t + 1$, so $H_{n,2t} \geq \sum_{j=0}^{t} \binom{2t+1}{j} = 2^c$. For $c = 2t + 1$, then $n \geq 2t + 2$, so $H_{n,2t+1} \geq 2\sum_{j=0}^{t} \binom{2t+1}{j} = 2^c$. Combining with $2^{n-m} \geq H_{n,c}$ yields $c \leq n - m$. Since $m \geq 2$, we have $n \geq c + 2$, so for $c = 2t$, $H_{n,2t} > \sum_{j=0}^{t} \binom{2t+1}{j} = 2^c$ and for $c = 2t + 1$, $H_{n,2t+1} > 2\sum_{j=0}^{t} \binom{2t+1}{j} = 2^c$. Combining with $2^{n-m} \geq H_{n,c}$ yields $c \leq n - m - 1$. □

V. Boolean correctors

This section investigates Boolean correctors whose correction order is optimal or suboptimal when considering nonlinear Boolean correctors. Indeed, the layer-profile characterization of Section III separates the corrector condition from nonlinearity optimization: once an admissible profile of layer support counts is fixed, the remaining degrees of freedom lie entirely in the intra-layer placement of support points to maximize nonlinearity. We exploit this decoupling across four directions. First, we classify all admissible layer profiles at correction orders $n - 1$ and $n - 2$ and establish a universal nonlinearity upper bound for $(n-2)$-correctors, complemented by a probabilistic existence bound for arbitrary profiles. Second, we construct an infinite family of self-addressing $(n - 2)$-correctors that achieves this nonlinearity upper bound whenever $n \geq 8$ is a power of two. Third, we generalize to constant-weight addressing to obtain explicit and asymptotically optimal $(n - d - 1)$-correctors for any fixed $d \geq 1$. Finally, we classify $(n - 3)$-correctors into two branches and characterize the limited parameters in injective Maiorana–McFarland (MM) constructions.

A. Classification of the highest correction orders

We begin by characterizing Boolean functions of maximum correction order $n - 1$ and next-to-maximum order $n - 2$ via their input layer profiles.

Proposition 2. *Every $(n-1)$-corrector is either the full parity function $x_1 + \cdots + x_n$ or its complement.*

Proof. If $A_0 = \cdots = A_{n-1} = 0$, $A_n(f) = P_f(1) = 2^n(-1)^{f(0)} = \pm 2^n$. Since there is only one element with Hamming weight n, Parseval's identity forces all remaining Walsh coefficients to be zero. Walsh inversion determines the function. Conversely, either of these affine functions has its sole nonzero Walsh coefficient at $\mathbf{1}$, so it has exact correction order $n - 1$. □

We now classify all Boolean functions of correction order $n - 2$. Because adding a constant 1 preserves both the correction order and the nonlinearity, it suffices to normalize $f(0) = 0$.

Theorem 4. *Let $n \geq 3$ and $f(0) = 0$, and suppose $f \in \mathcal{B}_n$ is neither the full parity function nor its complement. Then f is an $(n-2)$-corrector if and only if, for all $0 \leq w \leq n$,*

$$B_w(f) = \begin{cases} \binom{n-1}{w-1}, & w \text{ even}, \\ \binom{n-1}{w}, & w \text{ odd}. \end{cases} \tag{18}$$

or equivalently, $P_f(z) = 2^n z^{n-1}$.

Proof. Assume $P_f(z) = A_{n-1}z^{n-1} + A_n z^n$, then both $P_f(1) = A_{n-1} + A_n = 2^n$ and $P_f(-1) = (-1)^n(A_n - A_{n-1})$ belong to $\{2^n, -2^n\}$. It means that exactly one of A_{n-1}, A_n is zero and the other is 2^n. The solution with $A_n \neq 0$ would have order $n-1$, which is excluded. We therefore have $P_f(z) = 2^n z^{n-1}$. Eqs. (3) and (4) give $S_w = 2^{-n}\binom{n}{w}\frac{2^n}{n}K_{n-1}(w) = K_w(n-1)$. Hence, $\sum_w S_w(f)z^w = (1+z)(1-z)^{n-1}$, so

$$S_w = (-1)^w \left[\binom{n-1}{w} - \binom{n-1}{w-1} \right].$$

Substituting into $S_w(f) = \binom{n}{w} - 2B_w(f)$ proves Eq. (18). Conversely, computation from B_w gives exactly $A_{n-1} = 2^n$, ensuring that the correction order is exact $n-2$. □

Corollary 7. *For each* $0 \le w \le n$*, choose an arbitrary subset* $T_w \subseteq L_w^{(n)}$ *satisfying*

$$|T_w| = \begin{cases} \binom{n-1}{w-1}, & w \text{ even}, \\ \binom{n-1}{w}, & w \text{ odd}, \end{cases}$$

and define f_T *by* $\mathrm{supp}(f_T) = \bigcup_{w=0}^{n} T_w$*. Then* f_T *is an* $(n-2)$*-corrector, and the cardinality of the resulting family* $\mathcal{C}_n^{\max}$ *of normalized* $(n-2)$*-correctors is precisely* $|\mathcal{C}_n^{\max}| = \prod_{w=0}^{n} \binom{\binom{n}{w}}{|T_w|}$.

Corollary 8. *Every* $(n-2)$*-corrector satisfies*

$$M(f) \ge M_n^* := \max\left\{ 4\left\lceil \frac{2^{n-2}}{n} \right\rceil, 4\left(\lfloor 2^{n/2-2} \rfloor + 1 \right) \right\}, \qquad \mathrm{NL}(f) \le 2^{n-1} - \frac{1}{2}M_n^*. \tag{19}$$

The first term in the maximum dominates for all $n \ge 7$.

Proof. In the non-parity case, Theorem 4 gives a sum $\pm 2^n$ over the n Walsh coefficients at weight $n-1$. Therefore $M(f) \ge 2^n/n$, and four-divisibility strengthens this to $4\lceil 2^{n-2}/n \rceil$. Balancedness means $W_f(0) = 0$, so Parseval implies $(2^n - 1)M(f)^2 \ge 2^{2n}$, that is, $M(f) > 2^{n/2}$. Combining this strict inequality with four-divisibility supplies the other term. □

Because Corollary 7 only guarantees the correction order through the layer cardinalities $|T_w|$, we can search for highly nonlinear $(n-2)$-correctors by optimizing the intra-layer configuration of T_w. Specifically, a local search heuristic need only swap a support point $x \in T_w$ with a non-support point $y \in L_w \setminus T_w$ within the same layer, updating the Walsh spectrum via

$$W_{f'}(u) - W_f(u) = 2(-1)^{u\cdot x} - 2(-1)^{u\cdot y}.$$

Every function in Table I satisfies $(A_0, \ldots, A_n) = (0, \ldots, 0, 2^n, 0)$ and its nonlinearity achieves the nonlinearity upper bound of Eq. (19). Dimensions $n \le 10$ are cross-validated via integer programming models or exhaustive orbit search, whereas dimensions $11 \le n \le 16$ are obtained via cardinality-preserving incremental Walsh search.

TABLE I
$(n-2)$-CORRECTORS ACHIEVING THE NONLINEARITY UPPER BOUND $2^{n-1} - \frac{1}{2}M_n^*$ FOR $3 \le n \le 16$

n	c	M_n^*	NL	res	deg	n	c	M_n^*	NL	res	deg
3	1	4	2	0	2	10	8	104	460	0	9
4	2	8	4	0	2	11	9	188	930	0	10
5	3	8	12	0	3	12	10	344	1876	0	10
6	4	12	26	0	5	13	11	632	3780	0	11
7	5	20	54	0	6	14	12	1172	7606	0	13
8	6	32	112	0	6	15	13	2188	15290	0	14
9	7	60	226	0	8	16	14	4096	30720	0	14

Since the layer profile only focuses on how many support points belong to L_w, the nonlinearity may differ for different points in L_w. We can choose the supports uniformly, so the concentration inequality below applies to any admissible layer profile. It guarantees that there are many correctors whose Walsh coefficients lying close to their layer averages.

Theorem 5. *Let* $b = (b_0, \ldots, b_n)$ *be an admissible profile satisfying the conditions of Corollary 1, and define*

$$a_j = \sum_{w=0}^{n} \left(\binom{n}{w} - 2b_w \right) K_j(w), \qquad \mu(b) = \max_{0 \le j \le n} \frac{|a_j|}{\binom{n}{j}}.$$

Let $\mathcal{C}(b)$ be the family of Boolean functions with support counts $B_w(f) = b_w$. Then at least half of the functions in $\mathcal{C}(b)$ satisfy

$$M(f) \le \mu(b) + 2\sqrt{2^n(n+2)\ln 2}. \tag{20}$$

In particular, for any $1 \le \ell \le n-1$, the profile

$$b_w^{[\ell]} = \sum_{\substack{0 \le i \le \ell \\ i \text{ odd}}} \binom{\ell}{i}\binom{n-\ell}{w-i}. \tag{21}$$

satisfies $P_f(z) = 2^n z^\ell$ with $c(f) = \ell - 1$ and $\mu(b^{[\ell]}) = 2^n/\binom{n}{\ell}$. Consequently, at least half of the functions in $\mathcal{C}(b^{[\ell]})$ have correction order $\ell - 1$ and satisfy

$$\mathrm{NL}(f) \ge 2^{n-1} - \frac{2^{n-1}}{\binom{n}{\ell}} - \sqrt{2^n(n+2)\ln 2}.$$

Proof. For each $0 \le w \le n$, select a subset $T_w \subseteq L_w^{(n)}$ with $|T_w| = b_w$ uniformly at random and independently across layers. Define f by $\mathrm{supp}(f) = \bigcup_{w=0}^n T_w$, and it induces the uniform distribution on $\mathcal{C}(b)$. Fix $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) = j$, since the uniform distribution on $\mathcal{C}(b)$ is invariant under coordinate permutations, $\mathbb{E}[W_f(u)]$ depends only on j. Summing over all $\binom{n}{j}$ vectors of weight j yields $\mathbb{E}[W_f(u)] = a_j/\binom{n}{j}$.

Since $W_f(u) = 2^n \mathbf{1}_{\{u=0\}} - 2\sum_{w=0}^n \sum_{x \in T_w} (-1)^{u\cdot x}$, we define $Y_w(u) = \sum_{x\in T_w}(-1)^{u\cdot x}$, which is obtained by summing b_w values sampled without replacement from the set $\{(-1)^{u\cdot x} : x \in L_w\} \subset \{-1, 1\}$. Serfling's lemma [33, Theorem 2.2] says, for all $t \in \mathbb{R}$,

$$\mathbb{E}\left[\exp(t(Y_w(u) - \mathbb{E}[Y_w(u)]))\right] \le \exp\left(\frac{b_w t^2}{2}\right). \tag{22}$$

Let $Z(u) = W_f(u) - \mathbb{E}[W_f(u)]$, then using $W_f(u) = 2^n \mathbf{1}_{\{u=0\}} - 2\sum_{w=0}^n Y_w(u)$, the independence of the layer selections and Eq. (22) give

$$\mathbb{E}\left[\exp(tZ(u))\right] = \prod_{w=0}^n \mathbb{E}\left[\exp(-2t(Y_w(u) - \mathbb{E}[Y_w(u)]))\right] \le \prod_{w=0}^n \exp(2b_w t^2) = \exp(2^n t^2),$$

where the last equality uses the balance condition $\sum_w b_w = 2^{n-1}$. Applying the Chernoff bound [34] to both tails and optimizing over t gives, for any $t \in \mathbb{R}$,

$$\Pr\left(|Z(u)| \ge v\right) \le \left(\mathbb{E}[\exp(tZ(u))] + \mathbb{E}[\exp(-tZ(u))]\right)\exp(-tv) \le 2\exp\left(2^n\left(t - \frac{v}{2^{n+1}}\right)^2 - \frac{v^2}{2^{n+2}}\right) \le 2\exp\left(-\frac{v^2}{2^{n+2}}\right).$$

A union bound over all $u \in \mathbb{F}_2^n$ therefore gives

$$\Pr\left(\max_u |Z(u)| \ge v\right) \le \sum_{u\in\mathbb{F}_2^n} \Pr(|Z(u)| \ge v) \le 2^{n+1}\exp\left(-\frac{v^2}{2^{n+2}}\right).$$

Choosing $v = 2\sqrt{2^n(n+2)\ln 2}$ makes the right-hand side equal to $1/2$, hence, with probability at least $1/2$,

$$M(f) = \max_u |W_f(u)| \le \max_u |\mathbb{E}[W_f(u)]| + \max_u |W_f(u) - \mathbb{E}[W_f(u)]| \le \mu(b) + 2\sqrt{2^n(n+2)\ln 2}.$$

Since the sampling distribution is uniform on $\mathcal{C}(b)$, the first assertion follows.

For the particular case, let $\ell = c + 1$ and consider the linear Boolean function $g(x) = x_1 + \cdots + x_\ell$. Its support in L_w contains exactly

$$b_w^{[\ell]} = \sum_{\substack{0 \le i \le \ell \\ i \text{ odd}}} \binom{\ell}{i}\binom{n-\ell}{w-i}$$

vectors of weight w. Since the only nonzero Walsh coefficient of g is 2^n, occurring at $(\mathbf{1}_\ell, 0_{n-\ell})$, its Walsh layer-sum polynomial is $P_g(z) = 2^n z^\ell$. By Theorem 1, every function $f \in \mathcal{C}(b^{[\ell]})$ shares the same layer polynomial $P_f(z) = 2^n z^\ell$. Thus all members have exact correction order $c = \ell - 1$, and layer average $\mu(b^{[\ell]}) = 2^n/\binom{n}{\ell}$. Finally, applying the first assertion proves the nonlinearity bound. □

Take $c = n - d - 1$, Theorem 5 yields a family satisfying $P_f(z) = 2^n z^{n-d}$ and

$$M(f) \le \frac{2^n}{\binom{n}{d}} + 2\sqrt{2^n(n+2)\ln 2} = \frac{2^n}{\binom{n}{d}}\left(1 + O_d\left(n^{d+1/2}2^{-n/2}\right)\right).$$

Conversely, by the pigeonhole principle on layer $n-d$, every function with $P_f(z) = 2^n z^{n-d}$ satisfies $M(f) \geq 2^n/\binom{n}{d}$. Consequently, at least half of the functions in $\mathcal{C}(b^{[n-d]})$ satisfy

$$1 \leq \frac{M(f)}{2^n/\binom{n}{d}} \leq 1 + O_d\left(n^{d+1/2}2^{-n/2}\right), \tag{23}$$

demonstrating that the ratio converges to 1 as $n \to \infty$ for any fixed $d \geq 1$.

B. An optimal self-addressing family

We now show that the universal nonlinearity upper bound of Corollary 8 is achieved with equality by an infinite explicit family of self-addressing functions whenever $n \geq 8$ is a power of two.

Theorem 6. *Let $k \geq 3$, $n = 2^k$, and let π be a permutation on $\mathbb{F}_2^k$ with exactly one fixed point. For $x = (x_v)_{v\in\mathbb{F}_2^k} \in \mathbb{F}_2^n$, define*

$$L_\pi(x) = \sum_{v\in\mathbb{F}_2^k} x_v\pi(v), \quad g_\pi(x) = x_{L_\pi(x)}, \quad f_\pi(x) = \sum_{v\in\mathbb{F}_2^k} x_v + g_\pi(x).$$

Then f_π is an $(n-2)$-corrector with parameters

$$M(f_\pi) = \frac{2^n}{n}, \quad \mathrm{NL}(f_\pi) = 2^{n-1} - \frac{2^{n-1}}{n}, \quad \mathrm{res}(f_\pi) = \frac{n}{2} - 2, \quad \deg(f_\pi) = k+1 = \log_2 n + 1.$$

In particular, this family strictly achieves the nonlinearity upper bound of Corollary 8 for every $n = 2^k \geq 8$.

Proof. For $\alpha \in \mathbb{F}_2^k$, define $c_\alpha = (\alpha\cdot\pi(v))_{v\in\mathbb{F}_2^k}$, expand the address selector by orthogonality,

$$(-1)^{g_\pi(x)} = \sum_v \mathbf{1}_{\{L_\pi(x)=v\}}(-1)^{x_v} = \frac{1}{n}\sum_{\alpha,v}(-1)^{\alpha\cdot v}(-1)^{\alpha\cdot L_\pi(x)+x_v} = \frac{1}{n}\sum_{\alpha,v}(-1)^{\alpha\cdot v}(-1)^{(c_\alpha+e_v)\cdot x}.$$

Therefore,

$$W_{g_\pi}(u) = \frac{1}{n}\sum_{\alpha,v}\sum_x (-1)^{\alpha\cdot v}(-1)^{(c_\alpha+e_v+u)\cdot x} = \frac{2^n}{n}\sum_{\substack{\alpha,v\\ c_\alpha+e_v=u}}(-1)^{\alpha\cdot v}. \tag{24}$$

For nonzero α, $\mathrm{wt}(c_\alpha) = n/2$, as π is a permutation. If $c_\alpha + e_v = c_\beta + e_w$ with $\alpha \neq \beta$, then $c_{\alpha+\beta} = e_v + e_w$, which is a vector of weight $n/2 \geq 4$ with the number of ones at most two, a contradiction. Hence $c_\alpha + e_v = c_\beta + e_w$ yields $\alpha = \beta$ and $v = w$. Thus, the final sum in Eq. (24) contains at most one term, i.e., $W_{g_\pi}(c_\alpha + e_v) = \frac{2^n}{n}(-1)^{\alpha\cdot v}$. So $M(g_\pi) = 2^n/n$, and adding parity $\sum_v x_v$ does not change their Walsh magnitudes.

The term $\alpha = 0$ in Eq. (24) gives $u = e_v$ with Hamming weight 1, so $A_1(g_\pi) = \sum_{\mathrm{wt}(u)=1} W_{g_\pi}(u) = 2^n$. Consider the case $\alpha \neq 0$, we know $\mathrm{wt}(c_\alpha) = n/2$, then adding e_v only flips exactly one, i.e., the weight is $n/2-1$ if $\alpha\cdot\pi(v) = 1$, and $n/2+1$ otherwise. Thus, the Walsh support of g_π is on only three possible weight layers, $1, n/2-1$, and $n/2+1$. Assume

$$S_- = \sum_{\substack{\alpha\neq 0, v\in\mathbb{F}_2^k\\ \alpha\cdot\pi(v)=1}}(-1)^{\alpha\cdot v}, \quad S_+ = \sum_{\substack{\alpha\neq 0, v\in\mathbb{F}_2^k\\ \alpha\cdot\pi(v)=0}}(-1)^{\alpha\cdot v},$$

then $A_{n/2-1}(g_\pi) = \frac{2^n}{n}S_-$ and $A_{n/2+1}(g_\pi) = \frac{2^n}{n}S_+$. Indeed, $S_- + S_+ = \sum_{\alpha\neq 0}\sum_v (-1)^{\alpha\cdot v} = 0$. Their difference is

$$S_+ - S_- = \sum_v\sum_{\alpha\neq 0}(-1)^{\alpha\cdot(v+\pi(v))} = r(n-1) - (n-r) = n(r-1),$$

where r is the number of fixed points of π. Since $r = 1$, both middle-layer sums are zero and $P_{g_\pi}(z) = 2^n z$. Adding parity translates the entire Walsh spectrum by $\mathbf{1}_n$, thus, the weight layers are reversed $A_j(f_\pi) = A_{n-j}(g_\pi)$. Consequently,

$$P_{f_\pi}(z) = 2^n z^{n-1}, \quad c(f) = n-2.$$

Before adding parity, the nonzero Walsh coefficients occur at weights $1, n/2-1$, and $n/2+1$. After the parity, they occur at $n-1, n/2+1$, and $n/2-1$, where the smallest supported weight is $n/2-1$, therefore, $\mathrm{res}(f) = n/2-2$.

Write $L_\pi(x) = (L_1(x), \ldots, L_k(x))$, each address coordinate L_i is linear. Expanding the indicator,

$$g_\pi(x) = \sum_v x_v \prod_{i=1}^k (1 + L_i(x) + v_i),$$

so $\deg(g_\pi) \leq k+1$. Choose v_0 with $\pi(v_0) = 0$, then x_{v_0} does not appear in any L_i. Consequently

$$g_\pi(x) = x_{v_0}\prod_{i=1}^k (1 + L_i(x) + (v_0)_i) + R(x),$$

where $R(x)$ is independent of x_{v_0}. The first part, the selector $\mathbf{1}_{\{L(x)=v_0\}}$, has algebraic degree exactly k. To see this, choose w_i with $\pi(w_i)$ equal to the ith standard basis vector, and set all other variables to zero. It becomes $\prod_i(1+x_{w_i}+(v_0)_i)$, with nonzero term $x_{w_1}x_{w_2}\cdots x_{w_k}$. Thus multiplication by x_{v_0} supplies a degree-$(k+1)$ term that cannot cancel with the second part. Adding parity does not affect it. □

Remark 1. *The Walsh spectrum and algebraic degree derivations above hold for every permutation π. For π with r fixed points, the same calculation yields*

$$P_{f_\pi}(z) = 2^n z^{n-1} + 2^{n-1}(r-1)\left(z^{n/2-1} - z^{n/2+1}\right).$$

Thus, one fixed point is precisely the condition that removes the two unwanted layer sums in this construction. Whenever $r \neq 1$, the exact correction order drops to $n/2-2$.

Example 1. *Take $k=3$ and $n=8$. Identify each vector $v=(v_1,v_2,v_3)\in\mathbb{F}_2^3$ with the integer $i=v_1+2v_2+4v_3\in\{0,1,\ldots,7\}$, and write the input as $x=(x_0,x_1,\ldots,x_7)\in\mathbb{F}_2^8$. Define the permutation $\pi:\mathbb{F}_2^3\to\mathbb{F}_2^3$ by*

$$\pi(v_1,v_2,v_3) = (v_3,\ v_1+v_3,\ v_2),$$

which has cycle decomposition $(0)(1\ 2\ 4\ 3\ 6\ 7\ 5)$, so $v=0$ is its unique fixed point. Then the linear address map $L_\pi(x) = \sum_{v\in\mathbb{F}_2^3} x_v\pi(v) = (L_1(x),L_2(x),L_3(x))$ has

$$L_1(x) = x_4+x_5+x_6+x_7, \qquad L_2(x) = x_1+x_3+x_4+x_6, \qquad L_3(x) = x_2+x_3+x_6+x_7.$$

Thus, the resulting 8-variable self-addressing function is $f_\pi(x) = \sum_{i=0}^7 x_i + g_\pi(x) = \sum_{i=0}^7 x_i + x_{L_\pi(x)}$ with the hexadecimal truth table in least-significant-bit-first convention,

`299BA66A9A567A5195599E89A4D5569AA69554DA6E86655675A195A6A99A266B`

and has parameters

$$c(f_\pi)=6, \qquad M(f_\pi)=32, \qquad \mathrm{NL}(f_\pi)=112, \qquad \mathrm{res}(f_\pi)=2, \qquad \deg(f_\pi)=4,$$

achieving the universal nonlinearity upper bound of Corollary 8.

Our self-addressing construction achieves a better nonlinearity than $(n-2)$-correctors in [21, 22], as summarized in Table II. Indeed, the $(n-2)$-correctors in Zhang [21] have nonlinearity 2^{n-2}, which is strictly smaller than $2^{n-1}-2^{n-1}/n$ when $n\geq 8$. Meanwhile, Luo et al. [22, Theorem 1] constructed plateaued correctors of correction order $n-2$, with $\mathrm{NL}(f)=2^{n-1}-2^{n-l-1}$, $\mathrm{res}(f)=n-l-2$ and $\deg(f)=l+1$, subject to the structural constraint $n\geq 2^l+l$. Achieving our optimal nonlinearity $2^{n-1}-2^{n-1}/n$ within their framework would require $l=\log_2 n$, which violates their constraint $n\geq 2^l+l = n+\log_2 n$. Comparing Table II against Corollary 8 for $3\leq n\leq 16$, we see that the upper bound of Corollary 8 is achieved at $n=3,4$ by [21] and at $n=8,16$ by Theorem 6, whereas algebraic constructions obtaining M_n^* for non-power-of-two dimensions remain open.

TABLE II
PARAMETER COMPARISON OF $(n-2)$-CORRECTOR FAMILIES WITH WORK IN [21, 22]

Construction	Optimal nonlinearity	NL	deg	res	Constraint
Zhang [21]	✓[a]	2^{n-2}	2	$n-3$	–
Luo et al. [22]	×	$2^{n-1}-2^{n-l-1}$	$l+1$	$n-l-2$	$n\geq 2^l+l,\ n\geq 6$
Theorem 6	✓	$2^{n-1}-2^{n-1}/n$	$\log_2 n+1$	$n/2-2$	$n=2^k\geq 8$

[a] Only the cases $n=3,4$ meet the nonlinearity upper bound of Corollary 8.

C. An asymptotically optimal constant-weight addressing family

Whereas the self-addressing construction in Section V-B selects a single data bit, replacing that single bit with the parity of a constant-weight subset of data coordinates yields explicit constructions at any fixed distance $d\geq 1$ below the maximum correction order $n-1$. The following lemma decouples the spectral contribution of the s address variables from that of the t data variables.

Lemma 5. *Let $\phi:\mathbb{F}_2^s\to\mathbb{F}_2^t$ be a map of constant Hamming weight $\mathrm{wt}(\phi(y))=w$ for all $y\in\mathbb{F}_2^s$, and define $H:\mathbb{F}_2^s\times\mathbb{F}_2^t\to\mathbb{F}_2$ by $H(y,x)=h(y)+\phi(y)\cdot x$. Then for all $(a,b)\in\mathbb{F}_2^s\times\mathbb{F}_2^t$,*

$$W_H(a,b) = 2^t \sum_{y:\phi(y)=b} (-1)^{h(y)+a\cdot y}, \quad P_H(z) = 2^t z^w P_h(z). \tag{25}$$

If $h(y) = \ell \cdot y$ and $\mu = \max_b |\phi^{-1}(b)|$, then

$$P_H(z) = 2^{s+t} z^{w+\mathrm{wt}(\ell)}, \quad M(H) = 2^t \mu,$$

and every nonzero Walsh coefficient has data-weight w.

Proof. Sum over x first to obtain $W_H(a,b)$. Since $\mathrm{wt}(\phi(y)) = w$ for every $y \in \mathbb{F}_2^s$, $W_H(a,b)$ can be nonzero only when $\mathrm{wt}(b) = w$. Summing $W_H(a,b) z^{\mathrm{wt}(a)+\mathrm{wt}(b)}$ over $(a,b) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ therefore gives

$$P_H(z) = 2^t z^w \sum_{a \in \mathbb{F}_2^s} z^{\mathrm{wt}(a)} \sum_{y \in \mathbb{F}_2^s} (-1)^{h(y)+a\cdot y} = 2^t z^w P_h(z).$$

When $h(y) = \ell \cdot y$, the triangle inequality gives $|W_H(a,b)| \le 2^t |\phi^{-1}(b)| \le 2^t \mu$, with equality achieved at $a = \ell$ and any b realizing $\max_b |\phi^{-1}(b)|$. □

To maximize the correction order within this framework, we take $h(y)$ to be the full parity on the s address variables and let each address select the complement of a d-element subset of $\{1, \dots, t\}$.

Theorem 7. *Let $n = s + t$ with $1 \le d < t$, and let $\mathcal{S}$ be a map assigning to each address $y \in \mathbb{F}_2^s$ a d-element subset $S_y \subseteq \{1, \dots, t\}$. For $y = (y_1, \dots, y_s) \in \mathbb{F}_2^s$ and $x = (x_1, \dots, x_t) \in \mathbb{F}_2^t$, define*

$$f_{\mathcal{S}}(y, x) = \sum_{i=1}^{s} y_i + \sum_{j \notin S_y} x_j.$$

Let $\mu = \max_{S_y} |\mathcal{S}^{-1}(S_y)|$, then

$$c(f) = n - d - 1, \quad M(f) = 2^t \mu, \quad \mathrm{NL}(f) = 2^{n-1} - 2^{t-1}\mu.$$

Denote

$$\rho(\mathcal{S}) = \min \left\{ \mathrm{wt}(a) : \sum_{y \in \mathcal{S}^{-1}(S)} (-1)^{(\mathbf{1}_s + a)\cdot y} \neq 0 \text{ for some } S \right\}.$$

Then

$$\mathrm{res}(f) = t - d + \rho(\mathcal{S}) - 1, \qquad \deg(f) = 1 + \max_j \deg(\mathbf{1}_{\{j \notin S_y\}}) \le s + 1.$$

Furthermore, $\mathrm{res}(f) \le n - d - 2$ if and only if $\mathcal{S}$ is a nonconstant map.

Among all mappings for fixed (s, t, d), the minimum Walsh magnitude peak is

$$M_{s,t,d} = 2^t \left\lceil \frac{2^s}{\binom{t}{d}} \right\rceil,$$

which is achieved by any balanced map whose $|\mathcal{S}^{-1}(S_y)|$ differ by at most 1.

Proof. Let $\phi(y) = \mathbf{1}_t + \mathbf{1}_{S_y}$, so $\mathrm{wt}(\phi(y)) = t - d$, and $f(y, x) = \mathbf{1}_s \cdot y + \phi(y) \cdot x$. Lemma 5 determines the correction order and the minimum Walsh magnitude peak. The least possible address weight at a nonzero sum in Eq. (25) is precisely the number $\rho(\mathcal{S})$, therefore $\mathrm{res}(f) = t - d + \rho(\mathcal{S}) - 1$. The ANF is $\mathbf{1}_s \cdot y + \sum_j \mathbf{1}_{\{j \notin S_y\}} x_j$, terms involving different x_j cannot cancel, so the algebraic degree is determined.

In $\rho(\mathcal{S})$, $a = \mathbf{1}_s$ yields $\rho(\mathcal{S}) \le s$. Thus, suppose $\rho(\mathcal{S}) = s$, then for every $v \neq 0$, $\sum_{y \in \mathcal{S}^{-1}(S)} (-1)^{v\cdot y} = \sum_{y \in \mathbb{F}_2^s} \mathbf{1}_{\{\mathcal{S}(y)=S\}} (-1)^{v\cdot y} = 0$ for every S. Fourier inversion formula forces $\mathbf{1}_{\{\mathcal{S}(y)=S\}}$ to be constant for every $y \in \mathbb{F}_2^s$. Since every input y is mapped to exactly one subset, we have $\sum_{S \in \binom{[t]}{d}} \mathbf{1}_{\{\mathcal{S}(y)=S\}} = 1$ for all y, exactly one of them must equal 1, and all the others must equal 0. Hence there exists a unique S_0 such that $\mathbf{1}_{\{\mathcal{S}(y)=S_0\}} = 1$ for all y, i.e., $\mathcal{S}(y) = S_0$ for all y. Conversely, when $\mathcal{S}$ is constant, orthogonality makes $a = \mathbf{1}_s$ the only point contributing a nonzero sum, so $\rho = s$.

There are $\binom{t}{d}$ possible sets S_y, and the pigeonhole principle forces $\mu \ge \lceil 2^s / \binom{t}{d} \rceil$, equality is achieved by distributing the addresses as uniformly as possible among the subsets. Indeed, we have $2^s = q_0 \binom{t}{d} + r$ with $0 \le r < \binom{t}{d}$, assign $q_0 + 1$ addresses to r subsets and q_0 addresses to all the remaining subsets will achieve equality. Then all sizes differ by at most 1. □

Corollary 9. *Fix $d \ge 1$, and define*

$$D_d(n) = \sum_{\substack{0 \le r \le d \\ r \equiv d \pmod 2}} \binom{n}{r}, \quad T_d(n) = \frac{2^n}{D_d(n)}, \quad M_d^{\mathrm{addr}}(n) = \min_{1 \le s < n-d} M_{s,n-s,d}.$$

For every sufficiently large n, there is an explicit $(n-d-1)$-corrector with

$$1 \le \frac{M_d^{\mathrm{addr}}(n)}{T_d(n)} \le \frac{D_d(n)}{\binom{n-s}{d}} + \frac{D_d(n)}{2^s} = 1 + O_d\!\left(\frac{\log n}{n}\right),$$

where the asymptotic estimate is realized by choosing $s = \lceil (d+1)\log_2 n \rceil$. The resulting function has $\mathrm{res} \ge n-s-d-1$ *and* $\deg \le s+1$.

Proof. Every function in Theorem 7 satisfies $A_{n-d} = 2^n$. Averaging over that layer gives $M(f) \ge 2^n/\binom{n}{d} \ge T_d(n)$. While the right inequality arises from $M_{s,t,d} = 2^t \left\lceil 2^s/\binom{t}{d} \right\rceil$ and $\lceil x \rceil \le x+1$. Choosing $s = \lceil (d+1)\log_2 n \rceil$, for fixed d, we have

$$D_d(n) = \binom{n}{d}(1 + O_d(n^{-2})), \quad \frac{\binom{n}{d}}{\binom{n-s}{d}} = \prod_{i=0}^{d-1} \frac{n-i}{n-s-i} = 1 + O_d\left(\frac{s}{n}\right).$$

Theorem 7 supplies $\mathrm{res} \ge n-s-d-1$ and $\deg \le s+1$. □

For correction order $n-d-1$, the tail counts $D_{n,c}^{(i)}$ in Corollary 3 equal $D_d(n)$ and $D_d(n) - \binom{n-1}{d}$, respectively. Thus $T_d(n)$ is a universal lower bound on $M(f)$ for all $(n-d-1)$-correctors, and Corollary 9 shows that constant-weight addressing is asymptotically optimal with respect to this bound. In particular, since $T_1(n) = 2^n/n$, the $d=1$ family asymptotically meets the nonlinearity upper bound of Corollary 8 across all sufficiently large dimensions n. Representative parameters for $n \in \{64, 256, 1024\}$ are listed in Table III.

TABLE III
EXPLICIT PARAMETERS OF CONSTANT-WEIGHT ADDRESSING WITH $n = 64, 256, 1024$

n	d	s	t	μ	c	res $\ge$	deg $\le$	$M/T_d(n)$
64	1	10	54	19	62	52	11	1.1875
256	2	19	237	19	253	234	20	1.1829
1024	3	34	990	107	1020	986	35	1.1114

D. $(n-3)$-corrector classification

At correction order $n-3$, all Walsh layer sums below $n-2$ vanish, so the layer polynomial is supported on its three highest degrees: $n-2$, $n-1$, and n. The two evaluations $P_f(1)$ and $P_f(-1)$ then split the classification into two distinct branches, which Krawtchouk inversion translates into explicit layer-profile formulas. Throughout this subsection, binomial coefficients with an index outside its standard range are understood to be zero.

Let $B_w^{(1)}$ denote the $(n-2)$-corrector profile on the right-hand side of Eq. (18), and define

$$B_w^{(2)} = \begin{cases} 2\binom{n-2}{w-1}, & w \text{ even}, \\ \binom{n-2}{w} + \binom{n-2}{w-2}, & w \text{ odd}, \end{cases} \qquad \Delta_w = (-1)^w \binom{n-2}{w-1}.$$

Theorem 8. *Let $n \ge 5$ and $f(0) = 0$, then $f \in \mathcal{B}_n$ has exact correction order $n-3$ if and only if there exists*

$$\tau \in \{\pm 2^{n-1}, 0\} \tag{26}$$

such that exactly one of the following two branches holds,

Branch	$P_f(z)$	$B_w(f)$	*Condition*
I	$(2^n - \tau)z^{n-2} + \tau z^n$	$B_w^{(2)} - \frac{\tau}{2^{n-1}}\Delta_w$	$-$
II	$-\tau z^{n-2} + 2^n z^{n-1} + \tau z^n$	$B_w^{(1)} - \frac{\tau}{2^{n-1}}\Delta_w$	$\tau \ne 0$

(27)

Conversely, any profile $B_w(f)$ satisfying Eq. (27) *and $0 \le B_w(f) \le \binom{n}{w}$ generates a non-empty family of $(n-3)$-correctors within the corresponding branch.*

Furthermore, if $M(f) < 2^{n-1}$, only branch I with $\tau = 0$ occurs with $P_f(z) = 2^n z^{n-2}$ and $B_w(f) = B_w^{(2)}$. The resulting class $\mathcal{C}_n^{(n-3)}$ of normalized $(n-3)$-correctors with $\tau = 0$ has cardinality

$$|\mathcal{C}_n^{(n-3)}| = \prod_{w=0}^{n} \binom{\binom{n}{w}}{B_w^{(2)}}. \tag{28}$$

Proof. With all lower layers zero, write $P_f(z) = az^{n-2} + bz^{n-1} + \tau z^n$, so Walsh inversion at 0 and $\mathbf{1}_n$ gives

$$a + b + \tau = 2^n, \qquad (-1)^n(a - b + \tau) = 2^n(-1)^{f(\mathbf{1}_n)}.$$

Set $X = a + \tau$ and $Y = b$, then equations say $X + Y = 2^n$ and $X - Y = \pm 2^n$, therefore $(X, Y) = (2^n, 0)$ or $(0, 2^n)$. The two possibilities are

$$\mathrm{I} : P_f = (2^n - \tau)z^{n-2} + \tau z^n, \qquad \mathrm{II} : P_f = -\tau z^{n-2} + 2^n z^{n-1} + \tau z^n. \tag{29}$$

Their correction-order conditions are respectively $\tau \neq 2^n$ and $\tau \neq 0$. The Krawtchouk difference is $K_w(n) - K_w(n-2) = 4(-1)^w \binom{n-2}{w-1} = 4\Delta_w$, Eq. (4) and $B_w = (\binom{n}{w} - S_w)/2$ in the two possible cases of Eq. (29) gives exactly

$$\mathrm{I} : B_w = B_w^{(2)} - \frac{\tau}{2^{n-1}}\Delta_w, \qquad \mathrm{II} : B_w = B_w^{(1)} - \frac{\tau}{2^{n-1}}\Delta_w.$$

Since $\Delta_1 = -1$, integrality at $w = 1$ forces $\tau/2^{n-1} \in \mathbb{Z}$, so $|\tau| \leq 2^n$, as $\tau = W_f(\mathbf{1}_n)$. Furthermore, if $|\tau| = 2^n$, Parseval's identity forces it to be the parity function, so, these facts give the two possibilities in the theorem. The remaining restrictions $0 \leq B_w \leq \binom{n}{w}$ are necessary.

Conversely, any one of these vectors satisfying the number of support points can be realized by independent choices in each layer. The Krawtchouk transform is injective, so its layer polynomial is the specified one in Eq. (29). The coefficient at z^{n-2} is nonzero by the exclusion on τ proving exactness.

If $M(f) < 2^{n-1}$, the nonzero allowed values of τ are all impossible. Branch II then violates its exact-order condition, leaving only branch I with $\tau = 0$. Its class cardinality is $\prod_w \binom{\binom{n}{w}}{B_w^{(2)}}$ by independent selection. □

Corollary 10. *Every $(n-3)$-corrector $f \in \mathcal{B}_n$ with $n \geq 5$ satisfies*

$$M(f) \geq M^*_{n,3} := \max\left\{ 4\left\lceil \frac{2^{n-2}}{\binom{n}{2}} \right\rceil,\ 4\left(\left\lfloor 2^{\frac{n}{2}-2} \right\rfloor + 1\right) \right\}, \tag{30}$$

where the first term dominates for all $n \geq 13$.

Proof. In the case of $\tau = 0$, $A_{n-2} = 2^n$ is a sum of $\binom{n}{2}$ coefficients. Averaging and four-divisibility give $M \geq 4\left\lceil 2^{n-2}/\binom{n}{2} \right\rceil$. The strict balanced Parseval's identity supplies the second term. If $\tau \neq 0$, Theorem 8 gives $M \geq |\tau| \geq 2^{n-1}$, which is no smaller than the displayed lower bounds for $n \geq 5$. Hence the maximum of the two applies universally. □

Specializing Eq. (23) to $d = 2$ shows that at least half of the functions in $\mathcal{C}_n^{(n-3)}$ are asymptotically optimal with respect to Corollary 10. The proof follows from Theorem 5 with $\ell = n - 2$, so we omit it.

Corollary 11. *There exists an absolute constant $C > 0$ such that, for all sufficiently large n, at least half the functions in $\mathcal{C}_n^{(n-3)}$ satisfy*

$$M(f) \leq 4\left\lceil \frac{2^{n-2}}{\binom{n}{2}} \right\rceil + C2^{\frac{n}{2}}\sqrt{n} = \left(1 + O\left(n^{\frac{5}{2}}2^{-\frac{n}{2}}\right)\right) M^*_{n,3}.$$

Conjecture 1. *For every sufficiently large n, there exists $f \in \mathcal{C}_n^{(n-3)}$ with $M(f) = M^*_{n,3}$.*

For a prescribed bound $M \in 4\mathbb{Z}_{\geq 0}$, feasibility in the case of $\tau = 0$ can be expressed directly using binary variables $e_x \in \{0, 1\}$,

$$\sum_{x \in L_w} e_x = B_w^{(2)}, \quad 0 \leq w \leq n,$$
$$-M \leq 2^n \mathbf{1}_{\{u=0\}} - 2\sum_{x \in \mathbb{F}_2^n} e_x (-1)^{u \cdot x} \leq M, \quad u \in \mathbb{F}_2^n.$$

This system is feasible if and only if there is a function in $\mathcal{C}_n^{(n-3)}$ with maximum Walsh magnitude at most M. The strengthened integer model used for independent verification, including Parseval and all layer-sum equations, is given in Section B-B.

In Table IV, the $n = 7$ lower bound also uses the known covering radius $RM(1, 7) = 56$ [35], while Corollary 10 only gives $M^*_{7,3} = 12$.

TABLE IV
SPECTRAL AND NONLINEARITY BOUNDS FOR EXACT $(n-3)$-CORRECTORS

n	c	$M^*_{n,3}$	Achieved M	NL	res	deg	Status
5	2	8	8	12	0	3	Exact equality
6	3	12	12	26	0	5	Exact equality
7	4	16 (12)	16	56	0	4	Exact equality
8	5	20	24	116	0	6	Verified feasible
9	6	24	32	240	0	5	Injective MM
11	8	48	64	992	0	6	Injective MM

The $\tau = 0$ classification in Theorem 8 also imposes a structural limitation on the injective Maiorana–McFarland subclass.

Proposition 3. *Let $n = s + t \geq 5$ and let $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^t$ be injective. If $f(y, x) = \phi(y) \cdot x + h(y)$ is an $(n-3)$-corrector and $M(f) < 2^{n-1}$, then*

$$M(f) = 2^t, \qquad 2^s \leq \binom{n}{2}.$$

In particular, when $t = s + 1$, no injective MM semi-bent $(n-3)$-corrector exists for $s \geq 7$. More generally, an injective MM $(n-3)$-corrector can achieve the lower bound $M^*_{n,3}$ only when $M^*_{n,3}$ is a power of two.

Proof. By Lemma 5, $W_f(a, b) = 2^t \sum_{y:\phi(y)=b} (-1)^{h(y)+a\cdot y} \in \{0, \pm 2^t\}$ for all $(a, b) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$, so $M(f) = 2^t$. With $n = s+t$ and $M < 2^{n-1}$, Theorem 8 forces the function in the case of $\tau = 0$, up to complement. Consequently,

$$2^n = 2^{s+t} = |A_{n-2}(f)| \leq \binom{n}{2} 2^t.$$

If $t = s+1$, this becomes $2^s \leq s(2s+1)$. It fails at $s = 7$, and the ratio $2^s/[s(2s+1)]$ increases for $s \geq 7$, so it fails for every $s \geq 7$. Finally, every injective MM Walsh magnitude is a power of two, so equality with $M^*_{n,3}$ is possible in this subclass only when the bound itself equals a power of two. □

Thus the class with $P_f(z) = 2^n z^{n-2}$ provides asymptotically optimal $(n-3)$-correctors in every sufficiently large dimension, while the injective MM subclass is restricted to limited dimensions, in particular, the semi-bent case is impossible for $s \geq 7$.

VI. Vectorial correctors exceeding optimal linear correctors

A vectorial construction must control every nonzero component, not only its coordinate functions. This section develops a mechanism that enforces these conditions. Under a symmetric output preimage count $N_{w,b}$, every nonzero component function has the same layer polynomial, which significantly reduces the difficulty of the construction. Therefore, a preimage-layer-profile family that exceeds the optimal linear correctors is derived. On the other hand, since the preimage-layer-profile construction cannot control nonlinearity completely, a secondary construction uses finite-field addressing to control the Walsh coefficients. Every component function has the same constant-weight addressing, as field multiplication is a permutation. Therefore, the correction order and nonlinearity are separately controlled by base correctors and injectivity of address maps, respectively. Notably, Friedman [36] proved that for any (n, m, t)-resilient function, the resiliency t is bounded above by $t \leq \left\lfloor \frac{2^{m-1}n}{(2^m-1)} \right\rfloor - 1$, which implies our vectorial corrector's resiliency is strictly lower than its correction order. Table V summarizes these infinite families.

TABLE V
(n, m, c)-CORRECTORS WHOSE CORRECTION ORDER OUTPERFORMS THAT OF THE OPTIMAL LINEAR CORRECTORS

Construction	n	$m \geq$	c	NL	res
Theorems 9 and 10	$(2^m-1)s$	2	$2^{m-1}s + \ell - 1$	> 0	$0 \leq \text{res} \leq 2^{m-1}s - 2$
Theorem 12	$(2^m-1)(L+s)$	2	$2^{m-1}(L+s) + \ell - 1$	$2^{n-1} - 2^{n-n_0-1}$	$2^{m-1}L - 1$

A. A preimage-layer-profile family exceeding optimal linear correctors

For a vectorial function F, the corrector condition requires the vanishing of the Walsh layer sums $A_j(F_\lambda) = \sum_w S_w(F_\lambda) K_j(w)$ for all $j \leq c$ and $\lambda \neq 0$. Equivalently, in terms of the output preimage counts $N_{w,b}$, it imposes Krawtchouk moment constraints on each preimage, see Corollary 2. These constraints can be reduced if we impose a symmetry condition on those counts $N_{w,b}$, that is, for each input weight w, $N_{w,b}$ are all equal for every $b \neq 0$. Thus, $S_w(F_\lambda)$ are all equal for distinct $\lambda \neq 0$, and the construction of (n, m, c)-correctors then degenerates to a single profile $(S_0, \ldots, S_n)$ satisfying $\sum_w S_w K_j(w) = 0$ for $j \leq c$, whose corresponding $N_{w,b}$ are nonnegative integers.

Let $q = 2^m$, $n = (q-1)s$, and $d = qs/2$. A single-term profile $R_w = K_w^{(n)}(d + h)$, with $h > 0$, cannot be realized under this symmetry, as $a_1 = -\frac{2(q-1)h}{q} < 0$. We therefore consider two-term profile, for a positive even spacing ℓ,

$$R_w = \eta K_w^{(n)}(d + \ell) + (1 - \eta) K_w^{(n)}(d + 2\ell)$$

gives $a_1 = \frac{2(q-1)\ell(\eta-2)}{q}$. Note that ℓ cannot be odd, otherwise $a_{s,n} = \frac{1-3(q-1)}{q} < 0$. The boundary choice $a_1 = 0$ therefore yields $\eta = 2$, and it motivates the two-term profile below.

Construction 1. *Let $m \geq 2$ and $s \geq 1$ be integers. Let $q = 2^m$, $n = (q-1)s$, $d = qs/2$, and let ℓ be a positive even integer satisfying $d + 2\ell \leq n$. For $0 \leq w \leq n$, define*

$$R_{s,w} = 2K_w^{(n)}(d + \ell) - K_w^{(n)}(d + 2\ell),$$

and the rational counts

$$a_{s,w} = \frac{\binom{n}{w} + (q-1)R_{s,w}}{q}, \qquad b_{s,w} = \frac{\binom{n}{w} - R_{s,w}}{q}. \tag{31}$$

Whenever these counts are nonnegative integers, partition every input Hamming layer into one subset of size $a_{s,w}$ and $q-1$ subsets of size $b_{s,w}$. Assign the first subset to output 0 and the remaining subsets to the nonzero elements of $\mathbb{F}_2^m \setminus \{0\}$, every resulting map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ then satisfies

$$N_{w,0} = a_{s,w}, \qquad N_{w,b} = b_{s,w}, \quad b \in \mathbb{F}_2^m \setminus \{0\}.$$

Proposition 4. *Under Construction 1, if all counts $N_{w,b}$ are nonnegative integers, then every resulting map is an $(n, m, d+\ell-1)$-corrector.*

Proof. The defining formulas give $a_{s,w}+(q-1)b_{s,w} = \binom{n}{w}$, so the layer partitions exist. For every nonzero λ, we have $S_w(F_\lambda) = \sum_{b\in\mathbb{F}_2^m}(-1)^{\lambda\cdot b}N_{w,b} = a_{s,w} - b_{s,w} = R_{s,w}$, so Krawtchouk orthogonality (2) gives $A_j(F_\lambda) = 2^n(2\mathbf{1}_{j=d+\ell} - \mathbf{1}_{j=d+2\ell})$, which means the correction order is $d+\ell-1$. □

Thus the remaining construction problem is entirely a proof for nonnegative integers for (31). The next proposition treats their integrality, which has no restriction on the output dimension m.

Proposition 5. *Under Construction 1, all $a_{s,w}$ and $b_{s,w}$ with $0 \le w \le n$ are integers if and only if $q \mid 4\ell^2$.*

Proof. Let

$$G(t) = (1+t)^{n-d}(1-t)^d, \qquad \Delta_v(t) = (1+t)^v - (1-t)^v.$$

The generating identity gives

$$\mathcal{R}_s(t) := \sum_w R_{s,w}t^w = G(t) - (1+t)^{n-d-2\ell}(1-t)^d\Delta_\ell(t)^2. \tag{32}$$

The identity $j\binom{v}{j} = v\binom{v-1}{j-1}$ implies $2^{v_2(v)} \mid \binom{v}{j}$ when j is odd, so,

$$\Delta_v(t) = (1+t)^v - (1-t)^v = 2\sum_{\substack{1\le j\le v\\ j \text{ odd}}} \binom{v}{j} t^j \in 2^{1+\nu_2(v)}\mathbb{Z}[t].$$

If $q \mid 4\ell^2$, above equality gives $\Delta_\ell(t)^2 \in q\mathbb{Z}[t]$. Furthermore, $v = q/2$ with $\Delta_v(t)$ yields $(1+t)^{q/2} \equiv (1-t)^{q/2} \pmod q$, so

$$(1+t)^{q-1} = (1+t)^{q/2-1}(1+t)^{q/2} \equiv (1+t)^{q/2-1}(1-t)^{q/2} \pmod q.$$

Raising the congruence to the s-th power gives

$$(1+t)^n \equiv G(t) \pmod q. \tag{33}$$

Consequently,

$$\mathcal{R}_s(t) \equiv (1+t)^n \pmod q,$$

which proves integrality of $b_{s,w}$, and then $a_{s,w} = b_{s,w} + R_{s,w} \in \mathbb{Z}$.

Conversely, suppose all counts are integers, then $(1+t)^n - \mathcal{R}_s(t) \in q\mathbb{Z}[t]$. By Eqs. (32) and (33),

$$(1+t)^{n-d-2\ell}(1-t)^d\Delta_\ell(t)^2 = ((1+t)^n - \mathcal{R}_s(t)) - ((1+t)^n - G(t)) \in q\mathbb{Z}[t].$$

Since $\Delta_\ell(t)$ has constant coefficient zero and linear coefficient 2ℓ, while the other factor has constant coefficient one, the coefficient of t^2 is $4\ell^2$, so $q \mid 4\ell^2$. □

The shortest even spacing is $\ell = 2$. For this spacing, the integrality criterion becomes $q \mid 16$, which is equivalent to $2 \le m \le 4$. The corresponding profile is $R_{s,w} = 2K_w^{(n)}(d+2) - K_w^{(n)}(d+4)$. It therefore remains to establish the nonnegativity of all counts.

Theorem 9. *Let m, s be positive integers, $q = 2^m$, $n = (q-1)s$, and $d = qs/2$ with $2 \le m \le 4$, and*

$$s_0(m) = \begin{cases} 6, & m = 2, \\ 3, & m = 3, \\ 2, & m = 4. \end{cases}$$

Every realization in Construction 1 with $\ell = 2$ is an $(n, m, d+1)$-corrector for $s \ge s_0(m)$.

Proof. We choose the two-term as

$$R_{s,w} = 2K_w^{(n)}(d+2) - K_w^{(n)}(d+4), \tag{34}$$

and it remains to prove all $a_{s,w}$ and $b_{s,w}$ with $s \geq s_0(m)$ are nonnegative. Define the polynomials initially over $\mathbb{Q}$,

$$A_s(t) = \sum_{w=0}^{n} a_{s,w} t^w, \qquad B_s(t) = \sum_{w=0}^{n} b_{s,w} t^w, \qquad \mathcal{R}_s(t) = \sum_{w=0}^{n} R_{s,w} t^w.$$

We further define

$$H(t) = (1+t)^{q-1}, \qquad G(t) = (1+t)^{q/2-1}(1-t)^{q/2}.$$

Eq. (31) forces

$$A_s + (q-1)B_s = (1+t)^n, \qquad A_s - B_s = \mathcal{R}_s,$$

and by the definition of Krawtchouk (1), expanding Eq. (34) gives

$$\mathcal{R}_s(t) = \left[2\left(\frac{1-t}{1+t}\right)^2 - \left(\frac{1-t}{1+t}\right)^4\right](1+t)^{n-d}(1-t)^d,$$

so $\mathcal{R}_{s+1} = G\mathcal{R}_s$. Consequently,

$$\begin{cases} A_{s+1} + (q-1)B_{s+1} = H(A_s + (q-1)B_s), \\ A_{s+1} - B_{s+1} = G(A_s - B_s), \end{cases} \Rightarrow \begin{cases} A_{s+1} = UA_s + (q-1)VB_s, \\ B_{s+1} = VA_s + (U+(q-2)V)B_s, \end{cases}$$

where both

$$U = \frac{H + (q-1)G}{q}, V = \frac{H-G}{q} \in \mathbb{Z}_{\geq 0}[t],$$

as they are weight enumerators of the output preimage of a linear map [29]. Therefore, every nonnegative integer coefficients yields,

$$A_s, B_s \in \mathbb{Z}_{\geq 0}[t] \Longrightarrow A_{s+1}, B_{s+1} \in \mathbb{Z}_{\geq 0}[t].$$

And the fact, see Section A-A,

$$a_{s,w}, b_{s,w} \in \mathbb{Z}_{\geq 0}, \qquad s = s_0(m), \quad 0 \leq w \leq n,$$

then proves that every realization for such $a_{s,w}$ and $b_{s,w}$ is a $((q-1)s, m, qs/2+1)$-corrector. □

The preceding fixed-spacing profile cannot extend unchanged to $m \geq 5$, as for $\ell = 2$, $b_{s,2} = (\frac{q}{2}-1)s^2 + \frac{16}{q}$ is not integer. More generally, Proposition 5 requires $2^{\lceil m/2 \rceil - 1} \mid \ell$, which means ℓ must increase with m. The following result proves the high output dimension profile with certain conditions is sufficient, where Lemma 6 upper bounds the normalized Krawtchouk.

Lemma 6. *Let $a \geq 1$ and $b \geq 0$ be integers with $L = a + 2b$, and define*

$$\rho_w = \frac{[t^w](1+t)^a(1+t^2)^b}{\binom{L}{w}},$$

where $[t^w]f(t)$ is the coefficient of t^w in $f(t)$. Then $\rho_{L-w} = \rho_w$ and $\rho_0 \geq \rho_1 \geq \cdots \geq \rho_{\lfloor L/2 \rfloor}$. Consequently, if $n \geq 8$, $n/2 < j \leq n$, and $\alpha = 2j - n$, then

$$\frac{|K_w^{(n)}(j)|}{\binom{n}{w}} \leq \frac{\alpha^4 + 6n\alpha^2 + 3n^2}{n(n-1)(n-2)(n-3)}, \qquad 4 \leq w \leq n-4. \tag{35}$$

Proof. The polynomial $(1+t)^a(1+t^2)^b$ is palindromic of degree L, so $\rho_{L-w} = \rho_w$. We then prove the coefficient monotonicity by induction. First fix b and take $a = 1$, so $L = 2b+1$, then the coefficients at degrees $2i$ and $2i+1$ of $(1+t)^a(1+t^2)^b$ both equal $\binom{b}{i}$. Hence $\frac{\rho_{2i-1}}{\rho_{2i}} = 1$ for $1 \leq i \leq b$, and $\frac{\rho_{2i+1}}{\rho_{2i}} = \frac{2i+1}{L-2i} \leq 1$ for $i \leq \lfloor b/2 \rfloor$. Suppose the assertion holds for some $a \geq 1$, so multiplication by $1+t$ transforms a degree-L coefficient sequence into

$$\rho'_w = \frac{L+1-w}{L+1}\rho_w + \frac{w}{L+1}\rho_{w-1}, \qquad 1 \leq w \leq L,$$

with $\rho'_1 \leq \rho'_0$. For $2 \leq w \leq \lfloor \frac{L+1}{2} \rfloor$,

$$(L+1)(\rho'_{w-1} - \rho'_w) = (L+1-w)(\rho_{w-1} - \rho_w) + (w-1)(\rho_{w-2} - \rho_{w-1}).$$

Both terms are nonnegative before the middle, the central $\rho_w = \rho_{w-1}$ when L is odd follows from symmetry.

Now factor the Krawtchouk generating function, with $n/2 < j \leq n$ and $\alpha = 2j - n$,

$$K_w^{(n)}(j) = [t^w](1+t)^{n-j}(1-t)^j = [t^w](1-t)^\alpha(1-t^2)^{n-j},$$

so we obtain

$$|K_w^{(n)}(j)| \leq [t^w](1+t)^\alpha(1+t^2)^{n-j}.$$

Therefore, Eq. (35) follows from the monotonicity and symmetry $\rho_4 \geq \rho_w$ for $4 \leq w \leq n-4$ with $a = \alpha$ and $b = n - j$,

$$[t^4](1+t)^{\alpha}(1+t^2)^{n-j} = \binom{\alpha}{4} + \binom{\alpha}{2}(n-j) + \binom{n-j}{2} \leq \frac{\alpha^4 + 6n\alpha^2 + 3n^2}{24},$$

by removing all negative coefficients. □

Normalized Krawtchouk upper bounds in Lemma 6 will help us to prove the positivity of $a_{s,w}$ and $b_{s,w}$ with $3 \leq w \leq n-3$, which significantly reduces the proof of Theorem 10.

Theorem 10. *Let $m \geq 5$ and $s \geq 1$ be integers. Let $q = 2^m$, $n = (q-1)s$, $d = qs/2$, and let ℓ be a positive even integer satisfying $q \mid 4\ell^2$ and $16\ell^2 \leq qs^2$. Every realization in Construction 1 is an $(n, m, d+\ell-1)$-corrector.*

Proof. Since $q \mid 4\ell^2$ and $\ell \geq 2$, we have $s \geq 2$, so $n = s(q-1) \geq 62$. Furthermore, we have $2\ell \leq \frac{\sqrt{q}s}{2} \leq \frac{s(q-2)}{2} \leq n - d$, then Proposition 5 proves integrality of $a_{s,w}$ and $b_{s,w}$. Moreover, we know that

$$(a_{s,0}, b_{s,0}) = (1, 0), \qquad (a_{s,1}, b_{s,1}) = (0, s),$$

and

$$a_{s,2} = (q-1)\left(\binom{s}{2} - \frac{4\ell^2}{q}\right), \qquad b_{s,2} = s^2\left(\frac{q}{2} - 1\right) + \frac{4\ell^2}{q},$$

are all nonnegative as $q = 2^m \mid 4\ell^2$ and $\frac{4\ell^2}{q} \leq \frac{s^2}{4} \leq \binom{s}{2}$.

It remains to prove the nonnegativity of $a_{s,w}, b_{s,w}$ for $3 \leq w \leq n-3$. Indeed, Section A-B proves $(q-1)|R_{s,w}| < \binom{n}{w}$ for $3 \leq w \leq n-3$, it then follows that

$$\binom{n}{w} + (q-1)R_{s,w} > 0, \qquad \binom{n}{w} - R_{s,w} > 0.$$

Both $a_{s,w}$ and $b_{s,w}$ are positive, and together with integrality, this proves every realization is an exact $(n, m, d+\ell-1)$-corrector. □

Remark 2. *Different partitions of $N_{w,b}$ and assumptions of $R_{s,w}$ will lead to different (n, m, c)-correctors, for example, there exists a $(9, 3, 4)$-corrector, whose component layer polynomials are different, see Eq.* (44).

It can be proved $d_2((q-1)s, m) = qs/2$, which means our correction order exceeds the optimal linear correctors. However, the nonlinearity is hard to control since our constructions are based on the preimage counts, whereas the algebraic degree is also hard to determine.

Corollary 12. *The $(n, m, d+\ell-1)$-correctors in Theorems 9 and 10 with $n = (q-1)s$ and $d = qs/2$ exceed optimal linear correctors $d-1$, and*

$$0 \leq \mathrm{res}(F) \leq d-2, \qquad M_0 \leq M(F) < 2^n, \quad M_0 = \max\left\{\frac{2^{n+1}}{\binom{n}{d+\ell}}, \frac{2^n}{\binom{n}{d+2\ell}}, \frac{2^n}{\sqrt{2^n-1}}\right\}.$$

Proof. By Griesmer's bound [37], $g_m(d+1) = \sum_{i=0}^{m-1}\left\lceil\frac{d+1}{2^i}\right\rceil = \sum_{i=0}^{m-1}\left(\frac{d}{2^i}+1\right) = s(2^m-1)+m = n+m > n$, so, no binary $[n, m, d+1]$ linear code exists. On the other hand, repeating every column of a binary $[q-1, m, q/2]$ simplex generator matrix s times produces a binary $[n, m, d]$ linear code. Consequently, $d_2(n, m) = d$, and both correctors in Theorems 9 and 10 have correction order exceeding optimal linear correctors.

For each nonzero $\lambda \in \mathbb{F}_2^m$, the total influence [38] is given by

$$I(F_\lambda) = \sum_{i=1}^{n} \Pr(F_\lambda(X) \neq F_\lambda(X+e_i)) = 2^{-2n}\sum_{u\in\mathbb{F}_2^n} \mathrm{wt}(u)W_{F_\lambda}(u)^2,$$

where X is uniformly distributed on $\mathbb{F}_2^n$, and $e_1, \ldots, e_n$ denote the standard basis vectors. For every nonzero $v \in \mathbb{F}_2^m$, exactly $q/2$ vectors $\lambda \in \mathbb{F}_2^m \setminus \{0\}$ satisfy $\lambda \cdot v = 1$. Therefore,

$$\sum_{\lambda\neq 0} I(F_\lambda) = \frac{q}{2}\sum_{i=1}^{n} \Pr(F(X) \neq F(X+e_i)) \leq \frac{qn}{2} = (q-1)d. \tag{36}$$

Suppose, for a contradiction, that $\mathrm{res}(F) \geq d-1$. Then every nonzero component satisfies $W_{F_\lambda}(u) = 0$ whenever $\mathrm{wt}(u) < d$. Furthermore, $A_{d+\ell}(F_\lambda) = 2^{n+1} \neq 0$ ensures that at least one Walsh coefficient at weight $d+\ell$ is nonzero. Using Parseval's identity, it follows that $I(F_\lambda) > d$ for every $\lambda \neq 0$. Summing over the $q-1$ nonzero components contradicts Eq. (36), hence $\mathrm{res}(F) \leq d-2$. If all component Walsh coefficients at weight-one vanish, we can switch two points to make resiliency zero. Indeed, we have $a_{s,1} = 0$ and $b_{s,1} = s \geq 2$, therefore weight-one vectors $e_1, \ldots, e_n \in \mathbb{F}_2^n$ receive several different outputs. Choose e_i, e_j such that $F(e_i) \neq F(e_j)$, and choose a $\lambda \in \mathbb{F}_2^m$ satisfying $\lambda \cdot (F(e_i) + F(e_j)) = 1$. Then swapping the two

outputs changes the Walsh coefficient at frequency e_i by ± 4. Thus, there exists a realization with a nonzero weight-one Walsh coefficient, and hence with resiliency 0.

Fix a component function F_λ, if it is an affine function, then its layer polynomial would be $\pm 2^n z^j$ for some j. This is impossible because $P_{F_\lambda}(z) = 2^n \left(2z^{d+\ell} - z^{d+2\ell}\right)$ has two distinct nonzero terms. Therefore, $M(F) < 2^n$. Furthermore, every nonzero component F_λ has $P_{F_\lambda}(z) = 2^n(2z^{d+\ell} - z^{d+2\ell})$. The layer polynomial gives $A_{d+\ell}(F_\lambda) = 2^{n+1}$ and $A_{d+2\ell}(F_\lambda) = -2^n$. Thus, we have

$$2^{n+1} = \left| \sum_{\mathrm{wt}(u)=d+\ell} W_{F_\lambda}(u) \right| \le \sum_{\mathrm{wt}(u)=d+\ell} |W_{F_\lambda}(u)| \le \binom{n}{d+\ell} M(F),$$

and $2^n \le \binom{n}{d+2\ell} M(F)$. Combined with the Parseval's identity gives

$$M(F) \ge \max\left\{ \frac{2^{n+1}}{\binom{n}{d+\ell}}, \frac{2^n}{\binom{n}{d+2\ell}}, \frac{2^n}{\sqrt{2^n-1}} \right\}. \qquad \square$$

The output preimage counts give a deterministic realization of the corresponding vectorial function. For each $0 \le w \le n$, fix a lexicographic ordering $L_w = (x_{w,1}, \ldots, x_{w,\binom{n}{w}})$, and fix an ordering $\mathbb{F}_2^m \setminus \{0\} = \{\beta_1, \ldots, \beta_{q-1}\}$. Define F on L_w by assigning the first $a_{s,w}$ points to the output 0, and then assigning consecutive blocks of $b_{s,w}$ points to $\beta_1, \ldots, \beta_{q-1}$,

$$F(x_{w,j}) = \begin{cases} 0, & 1 \le j \le a_{s,w}, \\ \beta_\ell, & a_{s,w} + (\ell-1)b_{s,w} < j \le a_{s,w} + \ell b_{s,w}, \quad 1 \le \ell \le q-1. \end{cases}$$

It realizes the prescribed profile and therefore is an $(n, m, d+\ell-1)$-corrector. Switching two points x, y with different outputs $a \ne b$ in the same Hamming layer preserves $N_{w,b}$, so it preserves the correction order. For every nonzero component λ, the Walsh update is

$$\Delta W_{F_\lambda}(u) = \left((-1)^{\lambda\cdot b} - (-1)^{\lambda\cdot a}\right)\left((-1)^{u\cdot x} - (-1)^{u\cdot y}\right). \tag{37}$$

Hence every coefficient changes by only $0, \pm 4$, and repeating such swaps gives the following example, whose nonlinearity is lower than a general universal bound $\mathrm{NL}(F) \le 2^{n-1} - 2\left\lceil \frac{2^{n-2}}{\sqrt{2^n-1}} \right\rceil = 130814$ on nonlinearity of (n, m, c)-correctors by Parseval's identity. Also, it is 6 below the nonlinearity upper bound 130214 in Corollary 12.

Example 2. *At $(n, m, c) = (18, 2, 13)$, there exists a corrector with*

$$M(F) = 1728, \quad \mathrm{NL}(F) = 130208, \quad \mathrm{res}(F) = 0, \quad \deg(F) = 17.$$

Table VI presents parameters of the proposed vectorial correctors and compares their correction orders with those of optimal linear correctors at identical input and output dimensions. For $n = (2^m - 1)s$, the optimal linear correction order is $2^{m-1}s - 1$, whereas the proposed construction achieves correction order $2^{m-1}s + \ell - 1$ and resiliency at most $2^{m-1}s - 2$, yielding an exact improvement of $\ell \ge 2$.

TABLE VI
CORRECTION ORDER COMPARISON WITH OPTIMAL LINEAR CORRECTORS

(n, m)	s	ℓ	$c^{\mathrm{lin}}_{\max}$	$c(F)$	$\mathrm{res}(F) \le$	(n, m)	s	ℓ	$c^{\mathrm{lin}}_{\max}$	$c(F)$	$\mathrm{res}(F) \le$
$(18, 2)$	6	2	11	13	10	$(93, 5)$	3	4	47	51	46
$(21, 2)$	7	2	13	15	12	$(124, 5)$	4	4	63	67	62
$(24, 2)$	8	2	15	17	14	$(186, 5)$	6	8	95	103	94
$(27, 2)$	9	2	17	19	16	$(126, 6)$	2	4	63	67	62
$(21, 3)$	3	2	11	13	10	$(189, 6)$	3	4	95	99	94
$(28, 3)$	4	2	15	17	14	$(252, 6)$	4	8	127	135	126
$(35, 3)$	5	2	19	21	18	$(381, 7)$	3	8	191	199	190
$(42, 3)$	6	2	23	25	22	$(508, 7)$	4	8	255	263	254
$(30, 4)$	2	2	15	17	14	$(762, 7)$	6	16	383	399	382
$(45, 4)$	3	2	23	25	22	$(510, 8)$	2	8	255	263	254
$(60, 4)$	4	2	31	33	30	$(765, 8)$	3	8	383	391	382
$(75, 4)$	5	2	39	41	38	$(1020, 8)$	4	16	511	527	510

Zhang [21]'s construction is the closest nonlinear benchmark but its input dimension is $n = (q-1)s + m$, with output dimension m, where $q = 2^m$. [21, Theorems 2 and 4] has correction order $d = d_2(n, m) - 1$, resiliency $d - 1$, algebraic degree $m + 1$, and nonlinearity $2^{n-1} - 2^{n-m}$, while [21, Theorem 5] has the same correction order and algebraic degree, and

nonlinearity $2^{n-1} - 2^{n-m-1}$. The input dimension in [21] never meets our $(q-1)s$. To make the comparison dimension-consistent, we add identities for dimension matching, only slightly increase the correction order, resiliency and nonlinearity. That is, we define

$$F^+(x,y) = AF(x) + y, \qquad x \in \mathbb{F}_2^{(q-1)s}, \quad y \in \mathbb{F}_2^m,$$

where A is an invertible output linear transformation. Then $W_{(F^+)_\lambda}(u,v) = 2^m W_{F_{A^T\lambda}}(u)\mathbf{1}_{v=\lambda}$, which implies $P_{(F^+)_\lambda}(z) = 2^m z^{\mathrm{wt}(\lambda)} P_{F_{A^T\lambda}}(z)$. It therefore has correction order $c(F)+1$, resiliency $\mathrm{res}(F)+1$, algebraic degree $\deg(F)$, and nonlinearity $2^m\,\mathrm{NL}(F)$. The resulting comparisons establish a strict improvement in correction order. Note that this improvement only occurs

TABLE VII
COMPARISON AT COMMON DIMENSIONS $n = (2^m-1)s + m$ AND m OUTPUTS WITH $d = 2^{m-1}s$

Construction	c	res	deg	$\mathrm{NL}/2^{n-1}$
Optimal linear map	d	d	1	0
[21, Construction 2]	d	$d-1$	$m+1$	$1-2^{1-m}$
[21, Construction 3]	d	$d-1$	$m+1$	$1-2^{-m}$
F^+	$d+\ell$	$1 \le \mathrm{res} \le d-1$	$\deg(F)$	>0

in an admissible regime, that is,

(1) when $m = 2, 3, 4$, $s \ge s_0(m)$, see Theorem 9,
(2) when $m \ge 5$, $q \mid 4\ell^2$ and $16\ell^2 \le qs^2$, see Theorem 10.

Furthermore, our preimage layer profile constructions determine the component layer polynomials, but not every individual Walsh coefficient or algebraic degree. How to construct highly nonlinear (n,m,c)-correctors exceeding optimal linear correctors needs more investigation.

B. Finite-field realization of correctors with exact nonlinearity

The two-term corrector construction in the preceding two theorems describes the preimage layer profiles of every nonzero component function. It therefore determines the correction order, but it does not determine the individual Walsh coefficients of a realization. We now use an arbitrary realization as an address function in a finite-field construction. Nonzero field multiplication produces constant-weight addressing component, whose correction orders are determined by the chosen correctors and the constant-weight. Furthermore, the resulting function has an exact nonlinearity when the address maps are injective. Therefore, no assumption on the nonlinearity of the chosen address corrector is needed.

Let $m \ge 2$, $q = 2^m$, and fix an $\mathbb{F}_2$-linear isomorphism $\mathrm{vec} : \mathbb{F}_q \to \mathbb{F}_2^m$. For $a \in \mathbb{F}_q \setminus \{0\}$, define $c_a = (\mathrm{Tr}(av))_{v \in \mathbb{F}_q \setminus \{0\}} \in \mathbb{F}_2^{q-1}$, where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_2$ is the absolute trace, then the map $a \mapsto c_a$ is injective, and $\mathrm{wt}(c_a) = q/2$. Choose L address blocks of widths $r_1, \ldots, r_L$ with $n_0 = \sum_j r_j$ being the number of address variables, and set

$$\theta_j : \mathbb{F}_2^{r_j} \to \mathbb{F}_q \setminus \{0\}, \qquad \mu_j = \max_{a \in \mathbb{F}_q \setminus \{0\}} |\theta_j^{-1}(a)|.$$

For each $1 \le j \le L$ and each $v \in \mathbb{F}_q \setminus \{0\}$, assign one data variable $x_{j,v} \in \mathbb{F}_2$, thus $(q-1)L$ data variables accompany n_0 address variables. That is,

$$D_j(x) = \sum_{v \in \mathbb{F}_q \setminus \{0\}} x_{j,v} v,$$

and the total number of variables is $n = (q-1)L + n_0$. For an (n_0, m, c_H)-corrector H, use the trace-indexed components

$$H_\lambda(y) = \mathrm{Tr}\left(\lambda\, \mathrm{vec}^{-1}(H(y))\right), \qquad \lambda \in \mathbb{F}_q \setminus \{0\}.$$

Theorem 11. *Let H be an (n_0, m, c_H)-corrector, and define*

$$F_{H,\theta}(y,x) = H(y) + \mathrm{vec}\left(\sum_{j=1}^{L} \theta_j(y^{(j)}) D_j(x)\right). \tag{38}$$

Then, $F_{H,\theta}$ is an $(n, m, Lq/2 + c_H)$-corrector, with $n = L(q-1) + n_0$,

$$M(F_{H,\theta}) \le 2^{L(q-1)} \prod_{j=1}^{L} \mu_j, \qquad \mathrm{NL}(F_{H,\theta}) \ge 2^{n-1} - 2^{L(q-1)-1} \prod_{j=1}^{L} \mu_j.$$

$$\mathrm{res}(F_{H,\theta}) \ge \frac{Lq}{2} - 1, \qquad \deg(F_\lambda) = \max\{1 + \max_j \deg(\theta_j), \deg(H_\lambda)\}.$$

In particular, If, for every $1 \le j \le L$, there exists some $a \in \mathrm{Im}(\theta_j)$ such that $|\theta_j^{-1}(a)|$ is odd, then $\mathrm{res}(F_{H,\theta}) = Lq/2 - 1$. *Furthermore, if every θ_j is injective, then $F_{H,\theta}$ has*

$$M(F_{H,\theta}) = 2^{L(q-1)}, \qquad \mathrm{NL}(F) = 2^{n-1} - 2^{L(q-1)-1}, \qquad \mathrm{res}(F) = \frac{Lq}{2} - 1.$$

Proof. For simplicity, write $F = F_{H,\theta}$ and $B = L(q-1)$ for the number of data bits, so $n = B + n_0$. For $a \neq 0$, the binary vector $c_a = (\mathrm{Tr}(av))_{v \in \mathbb{F}_q \setminus \{0\}}$ has weight $q/2$, distinct nonzero a give distinct vectors. For each $\lambda \in \mathbb{F}_q \setminus \{0\}$, we have the component function

$$F_\lambda(y, x) = H_\lambda(y) + \Phi_\lambda(y) \cdot x,$$

where $\Phi_\lambda(y) = \left(c_{\lambda\theta_1(y^{(1)})}, \ldots, c_{\lambda\theta_L(y^{(L)})}\right)$, and $\mathrm{wt}(\Phi_\lambda(y)) = Lq/2$. Walsh transform at (u, b) is

$$W_{F_\lambda}(u, b) = 2^B \sum_{y : \Phi_\lambda(y) = b} (-1)^{H_\lambda(y) + u \cdot y}, \tag{39}$$

where each nonempty $\Phi_\lambda^{-1}(b) = \prod_j \theta_j^{-1}(\beta_j)$ with $b_j = c_{\lambda\beta_j}$, due to injectivity of $a \mapsto c_{\lambda a}$. Since the largest size of $\Phi_\lambda^{-1}(b)$ is $\prod_j \mu_j$, we have

$$M(F) \le 2^B \prod_{j=1}^{L} \mu_j, \qquad \mathrm{NL}(F) \ge 2^{n-1} - 2^{L(q-1)-1} \prod_{j=1}^{L} \mu_j.$$

And Lemma 5 tells us

$$P_{F_\lambda}(z) = 2^{L(q-1)} z^{Lq/2} P_{H_\lambda}(z), \tag{40}$$

which determines the correction order. Every nonzero coefficient (u, b) has data weight $\mathrm{wt}(b) = \mathrm{wt}(\Phi_\lambda) = Lq/2$, giving $\mathrm{res}(F) \ge Lq/2 - 1$.

Finally, expanding the data terms of F_λ yields

$$F_\lambda = H_\lambda(y) + \sum_{j=1}^{L} \sum_{v \in \mathbb{F}_q \setminus \{0\}} x_{j,v} \, \mathrm{Tr}(\lambda v \theta_j(y^{(j)})). \tag{41}$$

For each fixed $\lambda \neq 0$, the function $a \mapsto \mathrm{Tr}(\lambda v a)$ runs through all nonzero linear function, so one of them is therefore exactly has algebraic degree $d = \max_j \deg(\theta_j)$. Multiplication by data variable $x_{j,v}$ leads to a degree-$(d+1)$ monomial, and terms with distinct data variables cannot cancel. Since H_λ contains only address variables, it proves the algebraic degree.

Furthermore, if $|\theta_j^{-1}(\beta_j)|$ is odd for all $1 \le j \le L$, then $2^{-B} W_{F_\lambda}(u, b)$ is an odd sum of signs and cannot vanish for some b, so establish the exact resiliency $\mathrm{res}(F_{H,\theta}) = Lq/2 - 1$. The injectivity of θ_j for all j implies injectivity of Φ_λ, thus, Eq. (39) gives $|W_{F_\lambda}| = 2^B$, determining its nonlinearity. □

When θ_j is injective for all j, the nonlinearity and resiliency of $F_{H,\theta}$ are independent of the address corrector H, whose component values only determine the signs of the nonzero Walsh coefficients in Eq. (39), without their magnitudes. Thus, the two-term profiles in Theorems 9 and 10 can be realized on the address variables with exact nonlinearity, requiring no additional conditions. We call (m, s, ℓ) admissible when those results establish feasibility of $((q-1)s, m, qs/2 + \ell - 1)$-correctors in Theorems 9 and 10, that is, satisfying the following ranges,

(1) $2 \le m \le 4$: $\ell = 2$ and $s \ge s_0(m)$ with $(s_0(2), s_0(3), s_0(4)) = (6, 3, 2)$,
(2) $m \ge 5$: $q \mid 4\ell^2, 16\ell^2 \le qs^2$ with $s \ge 1$ and $\ell \ge 2$ even.

Theorem 12. *Let (m, s, ℓ) be admissible and let $q = 2^m$, $n_0 = (q-1)s$, and $d_0 = \frac{qs}{2}$. Choose any fixed two-term realization $H : \mathbb{F}_2^{n_0} \to \mathbb{F}_2^m$ such that*

$$P_{H_\lambda}(z) = 2^{n_0}(2z^{d_0+\ell} - z^{d_0+2\ell}), \qquad \lambda \in \mathbb{F}_q \setminus \{0\}. \tag{42}$$

Choose a decomposition $n_0 = \sum_{j=1}^{L} r_j$ with $1 \le r_j \le m-1$, and use injective addresses θ_j to construct $F_{H,\theta}$ by Eq. (38)*. Define*

$$n = (q-1)(L+s), \qquad d_* = \frac{(L+s)q}{2},$$

then $F_{H,\theta}$ is an $(n, m, d_* + \ell - 1)$-corrector with

$$M(F_{H,\theta}) = 2^{n-n_0}, \quad \mathrm{NL}(F_{H,\theta}) = 2^{n-1} - 2^{n-n_0-1}, \quad \mathrm{res}(F_{H,\theta}) = \frac{Lq}{2} - 1,$$
$$\deg(F_\lambda) = \max\{\deg(H_\lambda), \max_j \deg(\theta_j) + 1\},$$

where

$$c(F_{H,\theta}) - c_{\max}^{\mathrm{lin}}(n, m) = \ell, \qquad c(F_{H,\theta}) - \mathrm{res}(F_{H,\theta}) = \frac{qs}{2} + \ell. \tag{43}$$

Proof. For simplicity, use F to denote $F_{H,\theta}$, then substituting Eq. (42) into Eq. (40) gives $P_{F_\lambda}(z) = 2^n(2z^{d_*+\ell} - z^{d_*+2\ell})$ for $\lambda \neq 0$, so it proves the correction order. The injective-address gives the nonlinearity and resiliency, and algebraic degree follows from Theorem 11.

Every nonzero column of a dimension-m generator matrix contributes one to $q/2$ of its $q-1$ nonzero codeword weights. Hence, $d_2(n,m) \leq \frac{qn}{2(q-1)} = d_*$. Repeating every nonzero m-bit column exactly $s+L$ times achieves equality. Therefore $d_2(n,m) = d_*$ and $c^{\text{lin}}_{\max}(n,m) = d_* - 1$, which proves the first gap, and the second gap is immediate. □

When $\deg(H_\lambda) \leq \max_j r_j + 1$, the previous theorem already gives all correction order, nonlinearity, and resiliency independent of $\max_j \deg(\theta_j)$. We can vary its algebraic degree for a chosen block with maximum width to make $\deg(F_\lambda)$ varying from $\deg(H)$ to $\max_j \deg(\theta_j) + 1$.

Corollary 13. *Fix an (n_0, m, c_H)-corrector H and block widths $1 \leq r_j \leq m-1$, and let $R = \max_j r_j$. For every $1 \leq e \leq R$, the block addresses can be chosen injectively with $\max_j \deg(\theta_j) = e$.*

Proof. Fix an $\mathbb{F}_2$-basis $\xi_1, \ldots, \xi_m$ of $\mathbb{F}_q$, then choose the affine injection for each block $\mathbb{F}_2^{r_j}$,

$$\theta_j(y) = \xi_m + \sum_{i=1}^{r_j} y_i \xi_i, \qquad y \in \mathbb{F}_2^{r_j},$$

clearly its image avoids zero and in this case, $\max_j \deg(\theta_j) = 1$. For $2 \leq e < R$, choose any block of width R, compose its affine injection with

$$\sigma_e(y_1, \ldots, y_R) = (y_1 + y_2 \cdots y_{e+1}, y_2, \ldots, y_R).$$

Thus, the composition remains injective, has image avoiding zero, and has algebraic degree e. For $e = R \geq 2$, choose any block of width R, and define on it by a single-point change of θ_j,

$$\theta'_j(y) = \xi_m + \sum_{i=1}^{R} y_i \xi_i + (\xi_m + \xi_1) \prod_{i=1}^{R} (1 + y_i).$$

Thus the modified map remains injective into $\mathbb{F}_q \setminus \{0\}$ of algebraic degree R. Therefore $\max_j \deg(\theta_j)$ can take every value from 1 to R. □

Remark 3. *For fixed (n,m), the nonlinearity $2^{n-1} - 2^{n-n_0-1}$ with $n_0 = (q-1)s$ and $n = (q-1)(L+s)$ varies with distinct L. Since $n_0 = \sum_j r_j$ with $1 \leq r_j \leq m-1$, we obtain $L \geq \lceil n_0/(m-1) \rceil$, thus the maximum nonlinearity in Theorem 12 can be achieved by choosing the smallest $L = \lceil n_0/(m-1) \rceil$.*

We compare the proposed construction with optimal linear correctors and the nonlinear constructions of Zhang [21] in Table VIII. Throughout the comparison, the optimal linear correction order is $c^{\text{lin}}_{\max}(n,m) = d_2(n,m) - 1$. Note that each construction is evaluated at its own input dimension n, namely, $n = (2^m - 1)k + m$ for [21] and $n = (2^m - 1)(L+s)$ for Theorem 12, and n_0 is the input dimension of the base corrector H.

TABLE VIII
PARAMETER COMPARISON WITH NONLINEAR CORRECTORS AND LINEAR CORRECTORS

Construction	$c(F) - c^{\text{lin}}_{\max}(n,m)$	$\text{NL}(F)/2^{n-1}$	$c(F) - \text{res}(F)$	$\deg(F)$
Linear correctors	0	0	0	1
[21, Construction 2]	0	$1 - 2^{-m+1}$	1	$m+1$
[21, Construction 3]	0	$1 - 2^{-m}$	1	$m+1$
Theorem 12	ℓ	$1 - 2^{-n_0}$	$2^{m-1}s + \ell$	$\deg(H), \ldots, \max\{\deg(H), R+1\}$

Table VIII separates several improvements. First, the two-term address function provides the additive correction order advantage $c(F) - c^{\text{lin}}_{\max}(n,m) = \ell$. Second, injective addressing determines the exact nonlinearity, $\text{NL}(F)/2^{n-1} = 1 - 2^{-n_0}$, where $n_0 = (2^m - 1)s > m$. This nonlinearity formula is independent of those of the chosen realization of H. Theorem 12 also has a larger gap between correction order and resiliency. Finally, the algebraic degree of F can be determined by $\deg(H)$ and $\deg(\theta_j) \leq R$, with $R = \max_j r_j$.

Table IX gives concrete instances of the injective finite-field realization. The first column records the parameters of the correcting address function H, while the remaining columns describe the resulting function $F = F_{H,\theta}$. In each example, we choose the smallest number of $L = \lceil n_0/(m-1) \rceil$, and each block introduces $q-1$ data variables. Consequently,

$$n = n_0 + L(q-1), \qquad c(F) = c_H + \frac{Lq}{2},$$
$$\text{NL}(F) = 2^{n-1} - 2^{n-n_0-1}, \qquad \text{res}(F) = \frac{Lq}{2} - 1.$$

The four rows use $L = 18, 11, 10$, and 24, respectively. Thus the input expansion and all displayed spectral parameters follow from the same construction formulas.

TABLE IX
TWO-TERM CORRECTORS REALIZED BY AFFINE INJECTIVE ADDRESSES

(n_0, m, c_H)	(n, m)	$c(F)$	$c^{\mathrm{lin}}_{\max}(n, m)$	$\mathrm{NL}(F)$	$\mathrm{res}(F)$
$(18, 2, 13)$	$(72, 2)$	49	47	$2^{71} - 2^{53}$	35
$(21, 3, 13)$	$(98, 3)$	57	55	$2^{97} - 2^{76}$	43
$(30, 4, 17)$	$(180, 4)$	97	95	$2^{179} - 2^{149}$	79
$(93, 5, 51)$	$(837, 5)$	435	431	$2^{836} - 2^{743}$	383

VII. CONCLUSION

In this paper, we reformulated the Walsh criterion of correctors to the preimage profile across Hamming layers. We further gave nonlinearity upper bounds and correction order bounds for (n, m, c)-correctors. For Boolean correctors, nonlinear $(n-2)$- and $(n-3)$-correctors were fully characterized by the layer profiles. Furthermore, we constructed $(n-2)$-correctors achieving optimal nonlinearity, with resiliency $n/2-2$ and algebraic degree $k+1$ for $n = 2^k \geq 8$. Constructions of $(n-d-1)$-correctors that asymptotically meet the nonlinearity upper bounds for every fixed $d \geq 1$ were also derived. For vectorial correctors, nonlinear (n, m, c)-correctors whose correction order simultaneously outperforms that of the optimal linear corrector and its own resiliency were constructed by the preimage-layer-profile method. We also presented a secondary construction based on existing correctors, which preserves the correction-order advantage while providing an exact nonlinearity.

Determining the nonlinearity for (n, m, c)-correctors remains open, the optimal nonlinearity of (n, m, c)-correctors is currently characterized only for $m = 1$ and $c = n - 2$ with $n = 2^k \geq 8$. Constructing highly nonlinear vectorial correctors whose correction orders exceed the optimal linear correction order and its own resiliency remains an open problem.

ACKNOWLEDGEMENTS

The authors have used LLM-based tools (ChatGPT Astra, Gemini 4 Agron) to improve conciseness and phrasing. We are grateful to Yaoda Hu for pointing out several issues in an earlier version of the paper.

APPENDIX A
SUPPLEMENTAL PROOF

A. Initial nonnegative coefficients for the small-output profiles

For $q = 2^m$, $n = (q-1)s$, and $d = qs/2$ with $2 \leq m \leq 4$, we have

$$\mathcal{R}_s(t) = 2(1+t)^{n-d-2}(1-t)^{d+2} - (1+t)^{n-d-4}(1-t)^{d+4} = (1+t)^{n-d-4}(1-t)^{d+2}(1+6t+t^2).$$

Therefore,

$$A_s(t) = \frac{(t+1)^n + (q-1)\mathcal{R}_s(t)}{q}, \qquad B_s(t) = \frac{(t+1)^n - \mathcal{R}_s(t)}{q}.$$

For $(m, s) = (2, 6)$, we have $(q, n, d) = (4, 18, 12)$, for $(m, s) = (3, 3)$, we have $(q, n, d) = (8, 21, 12)$, for $(m, s) = (4, 2)$, we have $(q, n, d) = (16, 30, 16)$. The coefficient sequences $\{a_{s,w}\}$ and $\{b_{s,w}\}$ are palindromic because $d+2$ and $d+4$ are even. Thus, the entries for $0 \leq w \leq \lfloor n/2 \rfloor$, recorded in Table X, determine the full sequences. Each entry is a nonnegative integer, verifying the required initial feasibility.

B. Nonnegativity of $a_{s,w}$ and $b_{s,w}$ with $3 \leq w \leq n-3$ for large-output profiles

It is sufficient to prove that for $3 \leq w \leq n-3$, $(q-1)|R_{s,w}| < \binom{n}{w}$, where

$$q = 2^m \geq 32, \quad n = s(q-1), \quad d = \frac{qs}{2}, \quad q \mid 4\ell^2, \quad 16\ell^2 \leq qs^2.$$

Since $q \mid 4\ell^2$ and $\ell \geq 2$, we have $s \geq 2$, so $n = s(q-1) \geq 62$. Let $\beta_1 = s + 2\ell$, $\beta = s + 4\ell$, and $\rho = \beta/n$, then $16\ell^2 \leq qs^2$ gives

$$\rho = \frac{s+4\ell}{s(q-1)} \leq \frac{1+\sqrt{q}}{q-1} = \frac{1}{\sqrt{q}-1}, \qquad (q-1)\rho^2 \leq 1 + \frac{2}{\sqrt{q}-1}.$$

We first prove $w = 3$, since $K_3^{(n)}(j) = \frac{(n-2j)^3 - (3n-2)(n-2j)}{6}$, we have

$$6K_3^{(n)}(j) = (n-2j)^3 - (3n-2)(n-2j),$$

TABLE X
EXACT VALUES OF $a_{s,w}$ AND $b_{s,w}$ FOR $(m,s) = (2,6), (3,3), (4,2)$

	$(m,s)=(2,6)$		$(m,s)=(3,3)$		$(m,s)=(4,2)$	
w	$a_{s,w}$	$b_{s,w}$	$a_{s,w}$	$b_{s,w}$	$a_{s,w}$	$b_{s,w}$
0	1	0	1	0	1	0
1	0	6	0	3	0	2
2	33	40	7	29	0	29
3	336	160	287	149	370	246
4	204	952	532	779	1710	1713
5	3360	1736	2457	2556	8136	8958
6	3276	5096	7644	6660	38205	37038
7	8112	7904	13548	14676	129060	127116
8	12870	10296	24878	25516	360315	366174
9	9152	13156	38948	36426	894120	894202
10	–		42770	44278	1890750	1876951
11	–		–		3404910	3414826
12	–		–		5389620	5406907
13	–		–		7508880	7483398
14	–		–		9096615	9088404
15	–		–		9663480	9696936

therefore, $R_{s,3} = 2K_3^{(n)}(d+\ell) - K_3^{(n)}(d+2\ell)$ implies

$$6R_{s,3} = -(2\beta_1^3 - \beta^3) + (3n-2)(2\beta_1 - \beta) = -(2\beta_1^3 - \beta^3) + (3n-2)s.$$

As $0 < \beta_1^3 < \beta^3$ implies $|2\beta_1^3 - \beta^3| \le \beta^3$, we obtain

$$\frac{(q-1)|R_{s,3}|}{\binom{n}{3}} \le \frac{(q-1)\beta^3 + n(3n-2)}{n(n-1)(n-2)} \le \frac{(q-1)\rho^3 + \frac{3}{n}}{(1-\frac{1}{n})(1-\frac{2}{n})},$$

where $\rho = \beta/n$. Since $(1-\frac{1}{n})(1-\frac{2}{n}) \ge 915/961$, $(q-1)\rho^3 = ((q-1)\rho^2)\rho \le \frac{1}{4\sqrt{2}-1} \cdot (1 + \frac{2}{4\sqrt{2}-1})$, and $\frac{3}{n} \le \frac{3}{62}$, we have

$$\frac{(q-1)|R_{s,3}|}{\binom{n}{3}} < 1,$$

this ensures $a_{s,3}, b_{s,3} > 0$. And the symmetry $R_{s,n-3} = R_{s,3}$, derived from $K_{n-w}^{(n)}(j) = K_w^{(n)}(j)$ for both $d+\ell$ and $d+2\ell$ being even, gives the same conclusion at weight $n-3$.

For $4 \le w \le n-4$, since $n \ge 62$, $n/2 < d+\ell < d+2\ell \le n$, Lemma 6 gives

$$\begin{aligned}\frac{|R_{s,w}|}{\binom{n}{w}} &\le \frac{|2K_w^{(n)}(d+\ell)| + |K_w^{(n)}(d+2\ell)|}{\binom{n}{w}} \\ &\le \frac{2(\beta_1^4 + 6n\beta_1^2 + 3n^2) + \beta^4 + 6n\beta^2 + 3n^2}{n(n-1)(n-2)(n-3)} \\ &\le \frac{3(\beta^4 + 6n\beta^2 + 3n^2)}{n(n-1)(n-2)(n-3)},\end{aligned}$$

where $\beta_1 = s + 2\ell \le \beta = s + 4\ell$. Hence, we have

$$\frac{(q-1)|R_{s,w}|}{\binom{n}{w}} \le \frac{3(q-1)(\beta^4 + 6n\beta^2 + 3n^2)}{n(n-1)(n-2)(n-3)} = \frac{3(q-1)(\rho^4 + \frac{6\rho^2}{n} + \frac{3}{n^2})}{(1-\frac{1}{n})(1-\frac{2}{n})(1-\frac{3}{n})}.$$

Since the denominator is no less than $\frac{53985}{59582}$, and

$$\begin{aligned}3(q-1)\left(\rho^4 + \frac{6\rho^2}{n} + \frac{3}{n^2}\right) &= 3\big((q-1)\rho^2\big)\rho^2 + \frac{18(q-1)\rho^2}{n} + \frac{9(q-1)}{n^2} \\ &\le 3\left(1 + \frac{2}{4\sqrt{2}-1}\right)\left(\frac{1}{4\sqrt{2}-1}\right)^2 + \frac{18}{n}\left(1 + \frac{2}{4\sqrt{2}-1}\right) + \frac{9}{sn} \\ &\le 3\left(1 + \frac{2}{4\sqrt{2}-1}\right)\left(\frac{1}{4\sqrt{2}-1}\right)^2 + \frac{18}{62}\left(1 + \frac{2}{4\sqrt{2}-1}\right) + \frac{9}{124},\end{aligned}$$

we have

$$\frac{(q-1)|R_{s,w}|}{\binom{n}{w}} < 1, \qquad 4 \le w \le n-4.$$

Consequently,

$$a_{s,w} = \frac{\binom{n}{w} + (q-1)R_{s,w}}{q} > 0, \qquad b_{s,w} = \frac{\binom{n}{w} - R_{s,w}}{q} > 0, \qquad 3 \le w \le n-3.$$

APPENDIX B
SUPPLEMENTAL DATA

A. Small vectorial correctors achieving the universal nonlinearity bound

Corollary 2 derives the sufficient and necessary conditions for (n, m, c)-correctors, which concerns only the size of the preimage across Hamming layers. It gives freedom to switch points to search a higher nonlinearity, while preserving the correction order. That is, let x, y have the same Hamming weight, with $a = F(x)$ and $b = F(y)$, interchanging the two points changes the Walsh coefficients by Eq. (37), and has not influence on correction order.

Table XI contains four specified small vectorial correctors. The first three meet the universal bound on nonlinearity, the last is a feasible higher-order example, whose correction order is larger than the optimal linear correctors. The column headed "lower bound" is a proved lower bound on $M(F)$ for the indicated parameters.

TABLE XI
VERIFIED VECTORIAL CORRECTORS AND THEIR NONLINEARITY BOUNDS

(n, m, c)	Lower bound of M	Our M	NL	res	deg	Construction
$(5, 2, 1)$	8	8	12	0	2	Gold traces
$(7, 2, 2)$	16	16	56	0	2	Gold traces
$(5, 3, 1)$	8	8	12	0	3	Welch traces
$(9, 3, \mathbf{4})$	24	48	232	0	7	Joint profile

The Gold and Welch power functions are standard almost-bent constructions. They have the form $F(x) = (\mathrm{Tr}(\gamma_1 X^e), \ldots, \mathrm{Tr}(\gamma_m X^e))$ with $X = \sum_{i=1}^{n} x_i \beta_i \in \mathbb{F}_{2^n}$, where $e = 3$ for the two Gold examples and $e = 7$ for the Welch example. Here $(\beta_1, \ldots, \beta_n)$ is an ordered binary basis and the γ_i are binary linearly independent. The $(9, 3, 4)$-corrector in Table XI is specified by

$$\begin{aligned} &P_{F_\lambda}(z) = 512(2z^5 - z^7), && \lambda \in \{1, 5, 7\}, \\ &P_{F_\lambda}(z) = 512z^6, && \lambda \in \{2, 4, 6\}, \\ &P_{F_3}(z) = 512(-z^5 + 2z^7). \end{aligned} \tag{44}$$

Its correction order is therefore 4, and exceeds the linear-correction-order benchmark $d_2(9, 3) - 1 = 3$.

B. An integer model for $(n-3)$-correctors with $\tau = 0$

Let $B_w^{(2)}$ be the layer profile in Theorem 8 with $\tau = 0$, and let $M_0 \in 4\mathbb{Z}_{>0}$. To decide whether there exists a function $f \in \mathcal{C}_n^{(n-3)}$ with $M(f) \le M_0$, introduce a binary variable $y_x = f(x)$ for every $x \in \mathbb{F}_2^n$. For each nonzero $u \in \mathbb{F}_2^n$, introduce integer variables C_u and S_u. The existence problem can be formulated as the following finite-domain model

$$\sum_{x \in L_w} y_x = B_w^{(2)}, \qquad 0 \le w \le n, \tag{45}$$

$$C_u = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} y_x, \qquad u \ne 0, \tag{46}$$

$$(C_u, S_u) \in \left\{ (a, a^2) : a = -\frac{M_0}{2}, -\frac{M_0}{2} + 2, \ldots, \frac{M_0}{2} \right\}, \qquad u \ne 0, \tag{47}$$

$$\sum_{u \ne 0} S_u = 2^{2n-2}, \tag{48}$$

$$\sum_{u \in L_j} C_u = \sum_{w=0}^{n} B_w^{(2)} K_j^{(n)}(w), \qquad 1 \le j \le n. \tag{49}$$

Indeed, f is balanced, hence, for every $u \ne 0$,

$$W_f(u) = -2 \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} y_x = -2C_u.$$

Therefore, the allowed pairs in Eq. (47) are equivalent to $|W_f(u)| \leq M_0$. Eq. (48) is Parseval's identity divided by four, and Eq. (49) is the Krawtchouk layer-sum identity. Conversely, every function in $\mathcal{C}_n^{(n-3)}$ with maximum Walsh magnitude at most M_0 produces a feasible solution of Eqs. (45) to (49). Thus, the model is feasible if and only if such a function exists.

The model uses Python 3.14.5 and OR-Tools CP-SAT 9.15.6755, Windows 10 Enterprise LTS, Intel Core i9-10940X and 64GB, in 16 threads and random seed 20260905.

REFERENCES

[1] C. S. Petrie and J. A. Connelly, "A noise-based ic random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615–621, 2000.

[2] A. Hajimiri, S. Limotyrakis, and T. H. Lee, "Jitter and phase noise in ring oscillators," *IEEE Journal of Solid-state circuits*, vol. 34, no. 6, pp. 790–804, 1999.

[3] D. Kinniment and E. Chester, "Design of an on-chip random number generator using metastability," in *Proceedings of the 28th European Solid-State Circuits Conference*. IEEE, 2002, pp. 595–598.

[4] M. Sönmez Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," National Institute of Standards and Technology, Tech. Rep., 2016.

[5] ISO/IEC, "ISO/IEC 20543:2019: Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408," Geneva, 2019. [Online]. Available: https://www.iso.org/standard/68296.html

[6] W. Killmann and W. Schindler, "A proposal for: Functionality classes for random number generators," *ser. BDI, Bonn*, 2011.

[7] M. Grujić and I. Verbauwhede, "Optimizing linear correctors: A tight output min-entropy bound and selection technique," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 586–600, 2024.

[8] J. Von Neumann *et al.*, "Various techniques used in connection with random digits," *John von Neumann, Collected Works*, vol. 5, no. 768-770, p. 1, 1963.

[9] W. Hoeffding and G. Simons, "Unbiased coin tossing with a biased coin," *The Annals of Mathematical Statistics*, vol. 41, no. 2,341-352, 1970.

[10] M. Dwass, "Unbiased coin tossing with discrete random variables," *The Annals of Mathematical Statistics*, vol. 43, no. 3, pp. 860–864, 1972.

[11] P. Elias, "The efficient construction of an unbiased random sequence," *The Annals of Mathematical Statistics*, vol. 43, no. 3, pp. 865–870, 1972.

[12] Y. Peres, "Iterating von neumann's procedure for extracting random bits," *The Annals of Statistics*, pp. 590–597, 1992.

[13] M. Blum, "Independent unbiased coin flips from a correlated biased source—a finite state markov chain," *Combinatorica*, vol. 6, no. 2, pp. 97–108, 1986.

[14] A. Juels, M. Jakobsson, E. Shriver, and B. K. Hillyer, "How to turn loaded dice into fair coins," *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 911–921, 2000.

[15] H. Zhou and J. Bruck, "Efficient generation of random bits from finite state markov chains," *IEEE transactions on Information Theory*, vol. 58, no. 4, pp. 2490–2506, 2011.

[16] G. Seroussi and M. J. Weinberger, "Optimal algorithms for universal random number generation from finite memory sources," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1277–1297, 2014.

[17] R. B. Davies, "Exclusive or (xor) and hardware random number generators," *Retrieved May*, vol. 31, p. 2013, 2002.

[18] M. Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *International Workshop on Fast Software Encryption*. Springer, 2007, pp. 137–152.

[19] P. Lacharme, "Post-processing functions for a biased physical random number generator," in *International Workshop on Fast Software Encryption*. Springer, 2008, pp. 334–342.

[20] ——, "Analysis and construction of correctors," *IEEE transactions on Information Theory*, vol. 55, no. 10, pp. 4742–4748, 2009.

[21] W. Zhang, "Analysis and construction of nonlinear correctors used in true random number generators," *IEEE Transactions on Information Theory*, vol. 69, no. 10, pp. 6671–6681, 2023.

[22] S. Luo, W. Wang, Q. Zhang, and Z. Song, "Constructions of plateaued correctors with high correction order and good nonlinearity via walsh spectral neutralization technique," *Designs, Codes and Cryptography*, vol. 92, no. 12, pp. 4531–4548, 2024.

[23] Y. Hu, Y. Zhang, and W. Wu, "Construction of correctors using resilient fragmentary boolean functions," *Designs, Codes and Cryptography*, vol. 94, no. 1, p. 6, 2026.

[24] M. Grenouilloux, C. Li, and P. Méaux, "On the resilience order of weightwise almost perfectly balanced functions," in *International Workshop on the Arithmetic of Finite Fields*. Springer, 2026, pp. 199–220.

[25] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2020.

[26] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.)," *IEEE Transactions on Information Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[27] G. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Transactions on Information Theory*, vol. 34, no. 3, pp. 569–571, 1988.
[28] X.-M. Zhang and Y. Zheng, "Cryptographically resilient functions," *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1740–1747, 1997.
[29] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977, vol. 16.
[30] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of boolean functions with optimum algebraic immunity," *Designs, Codes and Cryptography*, vol. 52, no. 3, pp. 303–338, 2009.
[31] K. Suzuki and T. Iwata, "Bounds on fixed input/output length post-processing functions for biased physical random number generators," in *International Workshop on Selected Areas in Cryptography*. Springer, 2008, pp. 373–386.
[32] B. Chor, O. Goldreich, J. Hasted, J. Freidmann, S. Rudich, and R. Smolensky, "The bit extraction problem or t-resilient functions," in *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*, 1985, pp. 396–407.
[33] R. J. Serfling, "Probability inequalities for the sum in sampling without replacement," *The Annals of Statistics*, pp. 39–48, 1974.
[34] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *The Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 493–507, 1952.
[35] J. Mykkeltveit, "The covering radius of the (128, 8) reed-muller code is 56 (corresp.)," *IEEE Transactions on Information Theory*, vol. 26, no. 3, pp. 359–362, 1980.
[36] J. Friedman, "On the bit extraction problem," in *Annual Symposium on Foundations of Computer Science*, vol. 33, 1992, pp. 314–314.
[37] J. H. Griesmer, "A bound for error-correcting codes," *IBM Journal of Research and Development*, vol. 4, no. 5, pp. 532–542, 1960.
[38] R. O'Donnell, *Analysis of Boolean functions*. Cambridge University Press, 2014.