Symmetric Clusters in Hierarchy with Cryptographic Properties

Jeffrey Zheng

Abstract Symmetric Boolean functions play a key role in stream ciphers. Symmetric constructions provide core components in cryptographic applications. In this chapter, four meta symmetric clustering schemes (combination, crossing, variant and rotation) are organized in a hierarchy for n variables of 0–1 vectors in measuring phase spaces. Local counting properties in a cluster and global counting properties in a given level are formulated. From selected symmetric clusters, a number of various symmetric Boolean functions are formulated. Counting properties on symmetric clusters, vectors in selected clusters and special symmetric Boolean functions are listed. Four sets of symmetric Boolean functions are compared. Properties of symmetric clusters and Boolean functions are discussed. Main results are expressed in theorems and tables. Among four meta schemes, the variant scheme presents novel properties approximately with $O\left(n^2/4\right)$ clusters on a 2D phase space different from other schemes: combinatorial $O\left(n\right)$, crossing $O\left(n/2\right)$ and rotation $O\left(2^n/n\right)$ on 1D measuring phase spaces, respectively. The variant pseudorandom number generator is a similar approach on RC4 and HC128 stream ciphers using word-oriented 0–1 vectors. Further advanced researches and explorations on relevant optimal configurations are required.

Keywords Symmetric construction · Meta symmetric Cluster · hierarchy Boolean function · Four meta schemes · Phase space

This work was supported by the Key Project on Electric Information and Next Generation IT Technology of Yunnan (2018ZI002), NSF of China (61362014), Yunnan Advanced Overseas Scholar Project.

J. Zheng (✉)
Key Laboratory of Software Engineering of Yunnan, Kunming, China
e-mail: conjugatelogic@yahoo.com

J. Zheng (ed.), *Variant Construction from Theoretical Foundation to Applications*,
https://doi.org/10.1007/978-981-13-2282-2_5

1 Introduction

Symmetric Boolean functions [5] have being widely used as components of different cryptosystems [25] (e.g. in stream ciphers, block ciphers or hash functions). In combinatorial mathematics [10], a symmetric Boolean function is a Boolean function whose value does not depend on the permutation of its input bits [4], i.e. it depends only on the number of ones in the input on n variables of 0–1 vectors [21]. A total of 2^n vectors are composed of a vector space or a phase space for the construction [19]. For a specific symmetric Boolean function, it is necessary to have invariant properties undertaken a special group of permutations [18]. For example, rotation symmetric Boolean functions are invariant under the circular translation of indices. In addition to rotation symmetric properties, multiple invariants (combination, crossing, reflection, translation) may be composed of various symmetric subgroups of permutations [10, 22]. Various combinatorial counting schemes are explored [34–36].

1.1 Symmetric Functions—Combinatorial Invariant

From a combinatorial viewpoint, symmetric Boolean functions are a combinatorial invariant that links to the number of one elements $p, 0 \leq p \leq n$ in a vector [35]. In combinatorics, this type of function has being linked to binomial coefficients, and normally, there are $n + 1$ partitions to distinct the parameter of a measuring phase space into various clusters [30]. Symmetric Boolean functions are characterized [36] by the fact that their outputs only depend on the p numbers of their inputs. The usefulness of symmetric functions in a cryptographic context has being widely explored which possess good cryptographic properties [6, 7].

1.2 Crossing Number - Topological Invariant

A zero-crossing [23] describes a point where the sign of a mathematical function changes (e.g. from positive to negative), represented by a crossing of the axis (zero value) in the graph of the function. It is a commonly used term in electronics, mathematics, sound and image processing.

From a measuring viewpoint, a 0–1 vector with n bits can be expressed as a circular ring that has a fixed crossing number $q, 0 \leq q \leq \lfloor \frac{n}{2} \rfloor$ distinguished a number of derivative changes on either 0–1 or 1–0, respectively. This type of derivative invariant is widely used in crypto-analysis for many years. In NIST random data testing packages [1], binary derivative [3] and Runs tests [2] play an important role to measure the randomness of a binary sequence formed by a pseudorandom number generator for use in cipher systems. From an analytic viewpoint, this parameter is a

topological invariant and different from a combinatorial invariant to provide another type of partition capacities to organize a set of clusters in a measuring phase space.

1.3 Rotation Symmetric Functions - Geometric Invariant

In combinatorial mathematics, rotation symmetric properties are widely explored from early stage of abstract group theories and symmetric group constructions [10, 22] as a geometric invariant. Filiol and Fontaine [12] were initially explored on balanced Boolean functions with a good correlation immunity. Pieprzyk and Qu [26] were applied in crypto-applications to use Rotation Symmetric Boolean Functions (RSBF) as components in the rounds of a hashing algorithm.

Extensive R&D activities on RSBF are continuous for last decades, a list of advanced works explored, such as degree and non-linearity [6], optimal algebraic immunity [7], bent and semi-bent functions [8, 33], non-linearity of resilient, non-linear Boolean functions [20, 28], balanced Boolean functions [12, 16], non-linear balanced Boolean functions [31], weights and non-linearity [11], immune combining functions [32], count and cryptographic properties [13, 29], etc.

1.4 Trinomial Coefficients

It is a natural approach [10, 18, 19] to apply binomial coefficients to partition a measuring phase space on 0–1 vector sets. However, when parameters increase more than three, a generalization [34–36] using multinomial coefficients may not provide a general solution on further refined partitions, if the processed phase space is composed of 0–1 vectors. It is convenient for us to use a trinomial expression to show this fact.

Let $n = n_1 + n_2 + n_3, 0 < n$,

$$\binom{n}{n_1, n_2, n_3} = \frac{n!}{n_1! n_2! n_3!},$$

collecting all possible trinomial coefficients, we have

$$\sum_{\forall n_1, n_2, n_3} \binom{n}{n_1, n_2, n_3} = 3^n \neq 2^n. \tag{1}$$

From Eq. 1, it is interesting to notice that trinomial coefficients provide further segments to partition three-valued 0–2 vectors. Due to this reason, extensions using multinomial coefficients may not be directly relevant to binary-valued 0–1 vector sets. Refined identity equations of combinatorics are required [14, 15].

1.5 Variant Symmetric Schemes - Variant Invariants

Various schemes to use multiple invariants to partition special phase spaces have being explored in binary image analysis and processing for many years. In 1990s, Zheng [39, 40] proposed conjugate classifications to apply seven invariants in a hierarchy to partition the kernels of four regular plane lattices on $n = \{4, 5, 7, 9\}$ cases for 2D binary images. For n-tuple 0–1 vectors, variant logic frameworks [41, 42] are proposed in 2010s, various applications are explored, such as 3D visual method [37], variant Pseudorandom Number Generator (PRNG) [38, 43], computational simulation on quantum interactions [44–47] and non-coding DNA analysis [48–50].

1.6 Organization of the Chapter

In this chapter, an algebraic equation of variant trinomial will be proposed as a kernel structure to arrange a hierarchical phase space. This extension provides a general framework of multiple symmetric operations to support three numeric numbers: combinatorial, crossing and variant in a hierarchy. Three meta clusters of measuring phase spaces are identified by the three invariants: $\{n, p, q\}$ and their combinations. Refined levels can be compared with the rotation symmetric scheme under $n = \{1, 2, 3, 4, 5\}$ conditions. Similarities and differences among the four schemes are explored.

In Sect. 2, symbols and local counting properties of symmetric clusters in measuring spaces are defined, algebraic equations are formulated and two important projections are discussed. In Sect. 3, variant symmetric clusters and their elementary equation are proposed. In Sect. 4, four number sets of symmetric clusters are explored from a global viewpoint. In Sect. 5, symmetric Boolean functions of selected clusters are constructed and both algebraic and approximate numeric properties are discussed. In Sect. 6, cryptographic properties of symmetric Boolean functions in a hierarchy are discussed and special properties on the variant scheme are stressed. Section 7 is the conclusion of the chapter. Main results of the chapter are expressed in a list of theorems and corollaries in Sects. 2–5, respectively.

2 Symmetric Clusters in Measuring Phase Spaces

In this section, basic symbols, primary definitions and algebraic formulas are defined for different clusters in their measuring phase spaces.

2.1 Basic Symbols

Main symbols in this chapter are listed in Table 1.

2.2 Primary Definitions

Definition 1 (*x an n-tuple vector on 0–1 variables*) Let x be a 0–1 vector with n length.

$$x = (x_{n-1}, \ldots, x_i, \ldots, x_0), 0 \leq i < n, x_i \in \{0, 1\} = B_2, x \in B_2^n, \tag{2}$$

e.g. $x = 110010, n = 6$.

Table 1 Basic symbols

Symbol	Notes
n	Number of 0–1 variables, $1 \leq n$
x	0–1 vector $x = (x_{n-1}, \ldots, x_i, \ldots, x_0), x_i \in \{0, 1\} = B_2, 0 \leq i < n$
I	$I(x)$ index for a vector x
$\Omega(n)$	Phase space of vector set $\{x\}$, $\Omega(n) = \{\forall x \mid 0 \leq I < 2^n\}$
$f_\Omega(n)$	Number of vectors in $\Omega(n)$
R	$R(x, r)$ rotation operator
F	$F(x)$ reflection operator
p	$p(x)$ number of 1's elements in x, $0 \leq p \leq n$
q	$q(x)$ number of cyclic crossings either 0–1 or 1–0 in x
$L(p, n)$	Combinatorial cluster of vectors in $\Omega(n)$, $L(p, n) \subset \Omega(n)$
$E(q, n)$	Crossing cluster of vectors in $\Omega(n)$, $E(q, n) \subset \Omega(n)$
$V(q, p, n)$	Variant cluster of vectors in $\Omega(n)$, $V(q, p, n) \subset \Omega(n)$
$G(m, n)$	m-th rotation symmetric cluster of vectors in $\Omega(n)$, $G(m, n) \subset \Omega(n)$
$f_E(q, n)$	Crossing number of vectors in a cluster $E(q, n)$
$f_L(p, n)$	Combinatorial number of vectors in a cluster $L(p, n)$
$f(q, p, n)$	$f_V(q, p, n)$ variant number of vectors in a cluster $V(q, p, n)$
$f_G(m, n)$	Rotation number of vectors in the m-th cluster $G(m, n)$
$O(N)$	Approximate number of N
$C_X(n)$	Approximate number of clusters in a set of $\{X(.)\}$, $X \in \{E, L, V, G\}$
$f_X(n)$	Approximate number of clusters in a set of $\{X(.)\}$, $X \in \{E, L, V, G\}$
$SF_X(n)$	Number of Symmetric Boolean Functions (SBF) in $\{X(.)\}$, $X \in \{E, L, V, G\}$
$SF_{Xb}(n)$	Number of balanced SBF_X in $\{X(.)\}$, $X \in \{L, V, G\}$, $n = 0 \bmod 2$
$SF_{Eb}(n)$	Number of balanced SBF_E in $\exists q, \{E(q, n)\}$, $n = 0 \bmod 4$

Definition 2 (*I index for a vector x*) For a vector x, let I or $I(x)$ be an index:

$$I = I(x) = \sum_{i=0}^{n-1} x_i * 2^i, \tag{3}$$

e.g. $x = 110010$, $I(x) = 2^5 + 2^4 + 2 = 32 + 16 + 2 = 50$.

Definition 3 (*$\Omega(n)$ a full set of n-tuple 0–1 vectors*) Let $\Omega(n)$ be a vector space or a phase space of all n-tuple 0–1 vectors,

$$\Omega(n) = \{\forall x | 0 \leq I < 2^n, x \in B_2^n\} \text{ and } \Omega(n) = B_2^n. \tag{4}$$

Definition 4 Let $f_\Omega(n)$ denote a number of vectors in $\Omega(n)$.

Lemma 1 *$f_\Omega(n)$ is equal to 2^n.*

Proof For a vector $x \in B_2^n$ from $0 \ldots 0$ to $1 \ldots 1$, its index I can cover a full region of $0 \leq I < 2^n$, so $\Omega(n)$ contains 2^n distinct vectors and $f_\Omega(n) = 2^n$.

Definition 5 (*Measuring Phase Space*) If a phase space can be organized by various invariants, then it is a measuring phase space and its dimension is determined by a number of active invariants.

Corollary 1 *For any $n > 0$, $\Omega(n)$ is a measuring phase space in zero dimension.*

Proof For any $n > 0$, $\Omega(n)$ is composed of one cluster of vectors as a single point.

Definition 6 (*R rotation operator*) Let $R(x; r)$ be a rotation operator on a vector x rotation $-n < r < n$ positions:

$$\begin{aligned} R(x; r) &= R(x_{n-1}, \ldots, x_i, \ldots, x_0; r) \\ &= (x_{n-1+r \mod n}, \ldots, x_{i+r \mod n}, \ldots, x_{0+r \mod n}), \end{aligned} \tag{5}$$

e.g. $x = 110010$, $\{R(x; r)\}_{r=0}^5 = \{110010, 100101, 001011, 010110, 101100, 011001\}$ with six distinct vectors.

Lemma 2 (Maximal cyclic structure) *Initially from any vector x under a rotation operator, at most n distinct vectors will be distinguished under the rotation operator.*

Proof From any x, a set of $\{R(x; r)\}_{r=0}^{n-1}$ with n vectors can be generated. If the listed set of n vector sequences contains more than one cycle, then the number of distinct vectors will be less than n.

For example, $x = 110110$, $\{R(x; r)\}_{r=0}^5 = \{110110, 101101, 011011, 110110, 101101, 011011\}$ with only a set of three distinct vectors: $\{110110, 101101, 011011\}$.

Definition 7 (*F reflection operator*) Let $F(x)$ be a reflect operator,

$$F(x) = F(x_{n-1}, \ldots, x_i, \ldots, x_0) = (x_0, \ldots, x_i, \ldots, x_{n-1}), 0 \leq i < n. \quad (6)$$

Lemma 3 (A pair of reflections) *For any vector x, only two results are distinguished under $F(x)$ operation: (1) $F(x) = x$; (2) $F(x) \neq x$.*

Proof (1) If $F(x) = x$, then the values of the vector x are distributed as a central symmetric form; (2) if $F(x) \neq x$, then the vector x does not have a symmetric distribution.

For example, $x = 110010$, $F(x) = 010011$; $y = 110011$, $F(y) = 110011$.

Definition 8 (*p number of one elements*) Let p or $p(x)$ be a number of one elements in x,

$$p = p(x) = \sum_{i=0}^{n-1} x_i, 0 \leq p \leq n. \quad (7)$$

For example, $x = 110010$, $p(x) = 3$; $y = 110011$, $p(y) = 4$.

Definition 9 (*q number of cyclic crossings*) Let q or $q(x)$ be a number of cyclic crossings either 0–1 or 1–0 in a vector x,

$$\begin{aligned} q = q(x) &= \sum_{0 \leq i < n} (x_i \equiv 0) \& (x_{i+1} \equiv 1); x_i, x_{i+1} \in B_2, (i+1) \mod n; \\ &= \sum_{0 \leq i < n} (x_i \equiv 0) \& (x_{i-1} \equiv 1); x_i, x_{i-1} \in B_2, (i-1) \mod n; \\ & \qquad 0 \leq q \leq \lfloor \frac{n}{2} \rfloor. \end{aligned} \quad (8)$$

For example, $x = 110010$, $q(x) = 2$; $y = 110011$, $q(y) = 1$.

2.3 Counting Properties on Rotation Clusters

Definition 10 ($G(m, n)$ *m-th rotation symmetric cluster*) Let $G(m, n)$ be an m-th rotation symmetric cluster of vectors, $G(m, n) = \Omega(n|m) \subset \Omega(n)$ in $\Omega(n)$, and let a total number of rotation symmetric clusters be $C_G(n)$, $1 \leq m \leq C_G(n)$,

$$\Omega(n) = \bigcup_{m=1}^{C_G(n)} \Omega(n|m) = \bigcup_{m=1}^{C_G(n)} G(m, n). \quad (9)$$

Corollary 2 *A set of* $\{G(m,n)\}_{m=1}^{C_G(n)}$ *is composed of a measuring phase space in one dimension.*

Proof Using the parameter m, $\{G(m,n)\}_{m=1}^{C_G(n)}$ can be listed in a linear order.

Lemma 4 *By Burnside's lemma,* ϕ *being Euler's phi-function,*

$$C_G(n) = \frac{1}{n}\sum_{k|n}\phi(k)2^{\frac{n}{k}}. \tag{10}$$

Proof A brief proof of this lemma can be found in [29].

Definition 11 Let $f_G(m,n)$ denote a number of vectors in the m-th cluster $G(m,n)$.

Corollary 3 *For any* $f_G(m,n)$, $1 \le f_G(m,n) \le n$.

Proof Due to Lemma 2, each $f_G(m,n) \le n$ in general; for two special vectors in $\{0\ldots0, 1\ldots1\}$, we have $f_G(m,n) = 1$.

Corollary 4 *Collecting all possible rotation clusters, the total number of vectors is equal to* $f_\Omega(n)$

$$\begin{aligned}\sum_{m=1}^{C_G(n)} f_G(m,n) &= 2^n \\ &= f_\Omega(n).\end{aligned} \tag{11}$$

Proof From Lemma 4 and Corollary 3, it contains a full set of 2^n vectors in $\Omega(n)$.

Lemma 5 *For a given n,* $C_G(n)$ *has an approximate number,*

$$C_G(n) \approx O(\frac{2^n}{n}). \tag{12}$$

Proof Using Corollaries 3 and 4, each distinct cluster contains at most n vectors; it is a natural to have such an approximate number in enumeration.

It is convenient to list defined rotation parameters in Table 2 for $n = 4$ condition.

2.4 Counting Properties on Measuring Phase Spaces

For any vector $x \in \Omega(n)$, three measuring parameters $\{n, p, q\}$ are represented as three invariants. Three measurements transfer a phase space into a set of measuring phase spaces in a hierarchy.

Table 2 Six rotation clusters, various vectors in $\{G(m,4)\}$

(m,n)	$G(m,n)$	$f_G(m,n)$
(1, 4)	{0000}	1
(2, 4)	{0001, 0010, 0100, 1000}	4
(3, 4)	{0011, 0110, 1100, 1001}	4
(4, 4)	{0101, 1010}	2
(5, 4)	{0111, 1110, 1101, 1011}	4
(6, 4)	{1111}	1
	$C_G(4) = 6$	$f_\Omega(n) = 16$

Definition 12 ($L(p,n)$ *combinatorial cluster*) Let $L(p,n)$ be a combinatorial cluster of vectors in $\Omega(n)$, $L(p,n) = \Omega(n|p) \subset \Omega(n)$. Two parameters $\{n, p\}$ partition the phase space $\Omega(n)$ to form a set of clusters $\{L(p,n)\}$ in a measuring phase space.

$$\Omega(n|p) = L(p,n) = \{\forall x | 0 \leq p \leq n, x \in \Omega(n)\}. \tag{13}$$

Corollary 5 *A set of* $\{L(p,n)\}_{p=0}^{n}$ *is composed of a measuring phase space in one dimension.*

Proof The parameter p is the active invariant to arrange the phase space in a linear order.

Definition 13 Let $C_L(n)$ be a number of clusters in $\forall p, \{L(p,n)\}$.

Lemma 6 *For a given n,*

$$C_L(n) = n + 1. \tag{14}$$

Proof Using Definition 12, $0 \leq p \leq n$ and for any p, $L(p,n) \neq \emptyset$, the parameter p partitions the whole set $\Omega(n)$ into $n+1$ distinct subsets as clusters.

Definition 14 ($f_L(p,n)$ *combinatorial number*) Let $f_L(p,n)$ be a combinatorial number of vectors in a cluster $L(p,n)$.

Lemma 7 *For a pair of* $\{n, p\}$ *parameters,*

$$f_L(p,n) = \binom{n}{p} \tag{15}$$

Proof Using Definition 12, this number is equal to a binomial coefficient selected p elements from n positions.

It is convenient to list defined measuring parameters in Table 3 for $n = 4$ condition.

Table 3 Five clusters, various vectors in $\{L(p,4)\}$

(p,n)	$L(p,n)$	$f_L(p,n)$
(0, 4)	{0000}	1
(1, 4)	{0001, 0010, 0100, 1000}	4
(2, 4)	{0011, 0110, 1100, 1001, 0101, 1010}	6
(3, 4)	{0111, 1110, 1101, 1011}	4
(4, 4)	{1111}	1
	$C_L(4) = 5$	$f_\Omega(4) = 16$

Definition 15 ($E(q,n)$ *crossing cluster of vectors*) Let $E(q,n)$ be a crossing cluster of vectors in $\Omega(n)$, $E(q,n) = \Omega(n|q) \subset \Omega(n)$. Two parameters $\{n,q\}$ partition the phase space $\Omega(n)$ to form a set of clusters $\{E(q,n)\}$ in a measuring phase space.

$$\Omega(n|q) = E(q,n) = \{\forall x | 0 \le q \le \lfloor \frac{n}{2} \rfloor, x \in \Omega(n)\} \tag{16}$$

Corollary 6 *A set of* $\{E(q,n)\}_{q=0}^{\lfloor n/2 \rfloor}$ *is composed of a measuring phase space in one dimension.*

Proof The parameter q is the active invariant to arrange the phase space in a linear order.

Definition 16 Let $C_E(n)$ be a number of crossing clusters in $\forall q, \{E(q,n)\}$.

Lemma 8 *For a given* $n > 0$,

$$C_E(n) = \lfloor \frac{n}{2} \rfloor + 1. \tag{17}$$

Proof According to Definition 15 and each $E(q,n) \neq \emptyset, 0 \le q \le \lfloor \frac{n}{2} \rfloor$, the parameter q partitions the whole set $\Omega(n)$ into $\lfloor \frac{n}{2} \rfloor + 1$ distinct subsets as clusters.

Definition 17 ($f_E(q,n)$ *number of vectors*) Let $f_E(q,n)$ be a number of vectors in a cluster $E(q,n)$.

Lemma 9 *For a pair of* $\{n,q\}$ *parameters,*

$$f_E(q,n) = 2 * \binom{n}{2q}, 0 \le q \le \lfloor \frac{n}{2} \rfloor. \tag{18}$$

Proof Two cases can be distinguished: Case 1: $q = 0$; Case 2: $1 \le q \le \lfloor \frac{n}{2} \rfloor$.
Case 1: All n values are either 1 or 0, $2 * \binom{n}{0} = 2$.
Case 2: For a given q, $2q$ crossing positions are composed of a pair of a 0–1 crossing then a 1–0 crossing repeatedly for q times in a vector and this configuration has a total of $\binom{n}{2q}$ vectors included, and the same pair of positions can be exchanged as a

Table 4 Three clusters, vectors in $\{E(q,4)\}$ cases

(q,n)	$E(q,n)$	$f_E(q,n)$
(0, 4)	{0000, 1111}	2
(1, 4)	{0001, 0010, 0100, 1000, 0011, 0110, 1100, 1001, 0111, 1110, 1101, 1011}	12
(2, 4)	{0101, 1010}	2
	$C_E(4) = 3$	$f_\Omega(4) = 16$

pair of 1–0 and 0–1 crossings with the same number of different vectors, so a total of $2 * \binom{n}{2q}$ vectors are involved in each q selection.

It is convenient to list above defined measuring parameters in Table 4 for $n = 4$ condition.

3 Variant Symmetric Clusters

Definition 18 ($V(q,p,n)$ *variant cluster*) Let $V(q,p,n)$ be a variant cluster of vectors in $\Omega(n)$, $V(q,p,n) = \Omega(n|p,q) \subset \Omega(n)$. Three parameters $\{n,p,q\}$ partition the phase space $\Omega(n)$ to form a set of clusters $\{V(q,p,n)\}$ in a measuring phase space.

$$\Omega(n|p,q) = V(q,p,n) = \{\forall x | 0 \le p \le n, 0 \le q \le \lfloor \frac{n}{2} \rfloor, x \in \Omega(n)\} \quad (19)$$

Corollary 7 *A set of* $\{V(q,p,n)\}_{\forall q,p}$ *is composed of a measuring phase space on two dimensions.*

Proof Both invariants q and p are two active invariants to arrange the phase space on a 2D plane lattice.

Lemma 10 *Both* $\{L(p,n)\}$ *combinatorial clusters and* $\{E(q,n)\}$ *crossing clusters can be generated from special subsets of* $\{V(q,p,n)\}$ *variant clusters.*

Proof For a given p, $L(p,n)$ can be determined by

$$L(p,n) = \bigcup_{q=0}^{\lfloor \frac{n}{2} \rfloor} V(q,p,n).$$

For a given q, $E(q,n)$ can be determined by

$$E(q,n) = \bigcup_{p=0}^{n} V(q,p,n).$$

Table 5 Three sets of variant clusters for $n = 4$ in $\{V(q, p, n)\}$ condition

$q \backslash p$	0	1	2	3	4	$E(q,n)$
0	$V(0,0,4)$				$V(0,4,4)$	$E(0,4)$
1		$V(1,1,4)$	$V(1,2,4)$	$V(1,3,4)$		$E(1,4)$
2			$V(2,2,4)$			$E(2,4)$
$L(p,n)$	$L(0,4)$	$L(1,4)$	$L(2,4)$	$L(3,4)$	$L(4,4)$	$\Omega(4)$

Applying this set of partitions, three sets of relevant clusters can be identified.

For example, $n = 4$, all 16 vectors in the vector space, three sets of clusters can be distinguished as six clusters $\{V(q, p, n)\}$, five clusters for $\{L(p, n)\}$ and three clusters for $\{E(q, n)\}$ shown in Table 5, respectively.

Definition 19 Let $C_V(n)$ be a number of non-trivial variant clusters in $\forall q, p$, $\{V(q, p, n)\}$.

In general condition for any given $n > 1$, three sets of variant clusters could be shown in Fig. 1.

Theorem 1 *For a given n, $C_V(n)$ satisfies Eq. 20*

$$C_V(n) = \begin{cases} n^2/4 + 2; & n \equiv 0 \ mod\ 2 \\ (n^2 - 1)/4 + 2; & n \equiv 1 \ mod\ 2. \end{cases} \tag{20}$$

Proof From Fig. 1 for a given n, a triangular shape for non-trivial variant clusters is composed of two parts: a triangular area and two $q = 0$ points. The triangular

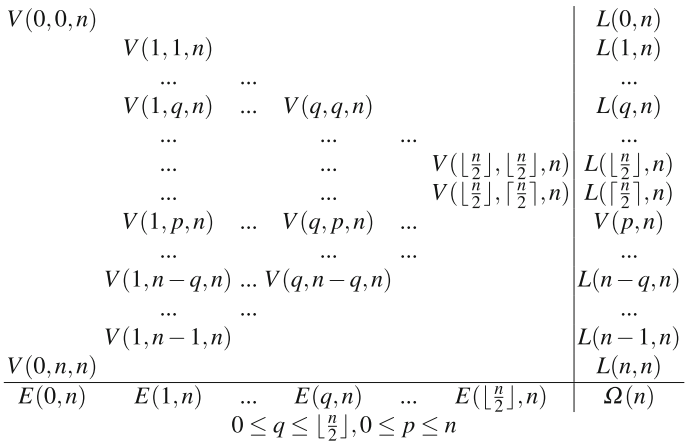

Fig. 1 Three sets of variant clusters $\{V(q, p, n)\}$, $\{E(q, n)\}$, $\{L(p, n)\}$ for $n > 1$

area has $(n-1)$ length and $\lfloor n/2 \rfloor$ high. If $n \equiv 0 \bmod 2$, the triangular area is a regular triangle contained $n^2/4$ clusters, so the total number of this triangular shape contains $n^2/4+2$ clusters. For an odd valued n, a triangular area has additional $\lfloor n/2 \rfloor$ clusters side on a regular triangle with $\lfloor n/2 \rfloor^2$ clusters, so the total number of clusters is $\lfloor n/2 \rfloor^2 + \lfloor n/2 \rfloor + 2 = (n^2-1)/4 + 2$.

3.1 Variant Trinomial Coefficients – Elementary Equation

Definition 20 Let $f_V(q, p, n)$ or $f(q, p, n)$ $0 \le p \le n, 0 \le q \le \lfloor \frac{n}{2} \rfloor$ denote an enumeration function for a number of 0–1 vectors in a variant cluster.

It is convenient to list relevant measuring parameters in Table 6 for $n = 4$ conditions.

Definition 21 For two initial and end clusters $p = \{0, n\}, q = 0$, let two cases be $f(0, 0, n) = f(0, n, n) = 1$. For other cases, each cluster $0 < p < n, 0 < q \le \lfloor \frac{n}{2} \rfloor$ contains a subgroup of vectors under a given condition. A variant trinomial coefficient for a number of vectors in a cluster is defined as an elementary equation in Equation 21,

$$f(q, p, n) = \frac{n}{n-p}\binom{n-p}{q}\binom{p-1}{q-1}. \tag{21}$$

Applying variant trinomial coefficients in Eq. 21, there is no difficult to process more complicated cases in enumeration. Global arrangements on their triangular shapes are convenient to be arranged by p measures in vertical direction. Two cases $n = \{4, 5\}$ are shown in Table 7.

In a general condition for any given $n > 1$, three sets of various numbers can be shown in Fig. 2.

Table 6 Six clusters, vectors in $\{V(q, p, 4)\}$

(q, p, n)	$V(q, p, 4)$	$f(q, p, 4)$
(0, 0, 4)	{0000}	1
(0, 4, 4)	{1111}	1
(1, 1, 4)	{0001, 0010, 0100, 1000}	4
(1, 2, 4)	{0011, 0110, 1100, 1001}	4
(1, 3, 4)	{0111, 1110, 1101, 1011}	4
(2, 2, 4)	{0101, 1010}	2
	$C_V(4) = 6$	$f_\Omega(4) = 16$

Table 7 Three sets of vector numbers $\{f(q,p,n)\}, \{f_E(q,n)\}, \{f_L(p,n)\}$;(a) $n=4$;(b) $n=5$

$p \backslash q$	0	1	2	$f_L(p,4)$
0	1			1
1		4		4
2		4	2	6
3		4		4
4	1			1
$f_E(q,4)$	2	12	2	$f_\Omega(4)=16$

(a) $n=4$

$p \backslash q$	0	1	2	$f_L(p,5)$
0	1			1
1		5		5
2		5	5	10
3		5	5	10
4		5		5
5	1			1
$f_E(q,5)$	2	20	10	$f_\Omega(5)=32$

(b) $n=5$

$$
\begin{array}{lllllll|l}
f(0,0,n) & & & & & & & f_L(0,n)\\
& f(1,1,n) & & & & & & f_L(1,n)\\
& \ldots & \ldots & & & & & \ldots\\
& f(1,q,n) & \ldots & f(q,q,n) & & & & f_L(q,n)\\
& \ldots & & \ldots & \ldots & & & \ldots\\
& \ldots & & \ldots & & f(\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor, n) & & f_L(\lfloor \frac{n}{2} \rfloor, n)\\
& \ldots & & \ldots & & f(\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil, n) & & f_L(\lceil \frac{n}{2} \rceil, n)\\
& f(1,p,n) & \ldots & f(q,p,n) & \ldots & & & f(p,n)\\
& \ldots & & \ldots & \ldots & & & \ldots\\
& f(1,n-q,n) & \ldots & f(q,n-q,n) & & & & f_L(n-q,n)\\
& \ldots & \ldots & & & & & \ldots\\
& f(1,n-1,n) & & & & & & f_L(n-1,n)\\
f(0,n,n) & & & & & & & f_L(n,n)\\
\hline
f_E(0,n) & f_E(1,n) & \ldots & f_E(q,n) & \ldots & f_E(\lfloor \frac{n}{2} \rfloor, n) & & f_\Omega(n)
\end{array}
$$

$$0 \le q \le \lfloor \tfrac{n}{2} \rfloor, 0 \le p \le n$$

Fig. 2 Three sets of $\{f(q,p,n)\}, \{f_E(q,n)\}, \{f(p,n)\}$ variant numbers for $n > 1$

3.2 Combinatorial Projection on Variant Clusters

From an algebraic viewpoint, the following theorems and corollaries are established for a general condition to meet any $n \ge 1$ cases.

Lemma 11 *If $f_L(p,n) = \sum_{q=1}^{p} f(q,p,n), 0 < p < n$, then the projection function $f_L(p,n)$ is a binomial coefficient and*

$$f_L(p,n) = \binom{n}{p}. \tag{22}$$

Proof For a fixed $p, 0 < p < n$, all possible $\{f(q,p,n)\}$ are collected to form the following combinatorial identities: [14, 15, 21],

$$
\begin{aligned}
f_L(p,n) &= \sum_{q=1}^{p} f(q,p,n) \\
&= \sum_{q=1}^{p} \frac{n}{n-p}\binom{n-p}{q}\binom{p-1}{q-1} \\
&= \frac{n}{n-p}\sum_{q=1}^{p}\binom{n-p}{q}\binom{p-1}{q-1} \\
&= \frac{n}{n-p}\sum_{q=1}^{p}\binom{n-p}{q}\binom{p-1}{p-q}; \quad \binom{N}{k} = \binom{N}{N-k} \\
&= \frac{n}{n-p}\binom{n-1}{p}; \quad \binom{x+y}{N} = \sum_{k=0}^{N}\binom{x}{k}\binom{y}{N-k} \\
&= \frac{n}{(n-p)}\frac{(n-1)!}{(n-p-1)!p!} \\
&= \frac{n!}{(n-p)!p!} \\
&= \binom{n}{p}.
\end{aligned}
$$

For a complete sequence of binomial coefficients, it is necessary to include both initial and end clusters. Further Theorem 2 can be established.

Theorem 2 *For any given $n > 0$, a set of projection function $\{f_L(p,n)\}_{p=0}^{n}$ is composed of the same sequence of binomial coefficients*

$$f_L(p,n) = \binom{n}{p}. \tag{23}$$

Proof For $0 < p < n$ condition, the equation has been determined by Lemma 11 and two end clusters $p = \{0, n\}$, $\binom{n}{0} = \binom{n}{n} = 1$ are determined by Definition 21.

Corollary 8 *The sum of all possible $\{f_L(p,n)\}_{p=0}^{n}$ is equal to $f_\Omega(n)$,*

$$\sum_{p=0}^{n} f_L(p,n) = f_\Omega(n) = 2^n. \tag{24}$$

Proof Collecting all possible numbers in Theorem 2, we have

$$\begin{aligned}\sum_{p=0}^{n} f_L(p,n) &= \sum_{p=0}^{n} \binom{n}{p} \\ &= (1+1)^n \\ &= 2^n \\ &= f_\Omega(n).\end{aligned}$$

3.3 Crossing Projection on Variant Clusters

Lemma 12 *If* $f_E(q,N) = \sum_{p=q}^{n-q} f(q,p,n)$, $1 \le q \le \lfloor \frac{n}{2} \rfloor$, *then the enumeration function* $f_E(q,n)$ *is a double of a binomial coefficient*

$$f_E(q,n) = 2\binom{n}{2q}. \tag{25}$$

Proof For a fixed q, collecting all possible $\{f(q,p,n)\}_{p=q}^{n-q}$, the following combinatorial identities [14, 15, 21] are deduced:

$$\begin{aligned}f_E(q,n) &= \sum_{p=q}^{n-q} f(q,p,n) \\ &= \sum_{p=q}^{n-p} \frac{n}{n-p}\binom{n-p}{q}\binom{p-1}{q-1} \\ &= \sum_{p=q}^{n-p} \frac{n}{q}\binom{n-p-1}{q-1}\binom{p-1}{q-1}; \quad \frac{N}{q}\binom{N-p-1}{q-1} = \frac{N}{N-p}\binom{N-p}{q} \\ &= \frac{n}{q}\sum_{p=q}^{n-p}\binom{n-p-1}{q-1}\binom{p-1}{q-1}\end{aligned}$$

$$= \frac{n}{q}\binom{n-1}{2q-1}; \quad \binom{N+1}{r+s+1} = \sum_{k=r}^{N-s}\binom{k}{r}\binom{N-k}{s}$$
$$= 2\frac{n}{2q}\frac{(n-1)!}{(n-2q)!(2q-1)!}$$
$$= 2\frac{n!}{(2q)!(n-2q)!}$$
$$= 2\binom{n}{2q}.$$

Theorem 3 *For any given $n > 0$ under the listed condition, a set of projection function $\{f_E(q,n)\}_{0\le q\le\lfloor\frac{n}{2}\rfloor}$ are composed of the subsequence of binomial coefficients,*

$$f_E(q,n) = 2\binom{n}{2q}. \tag{26}$$

Proof For $1 \le q \le \lfloor n/2 \rfloor$ condition, equations are determined by Lemma 12 and for the initial subgroup, we have $q = 0$, $f_E(0,n) = \binom{n}{0} + \binom{n}{n} = 2\binom{n}{0}$.

Corollary 9 *For $n \equiv 0 \mod 2, 0 \le q \le n/2$, there are a pair of symmetric functions*

$$f_E(q,n) = f_E(n/2-q,n). \tag{27}$$

Proof Under $n \equiv 0 \mod 2$ condition,

$$\begin{aligned} f_E(q,n) &= 2\binom{n}{2q} \\ &= 2\binom{n}{n-2q} = 2\binom{n}{2(n/2-q)} \\ &= f_E(n/2-q,n). \end{aligned}$$

Corollary 10 *For $n \equiv 0 \mod 4, q = n/4$, $f_E(n/4,n)$ has the maximal value*

$$f_E(n/4,n) > f_E(q,n), q \ne n/4. \tag{28}$$

Proof Under $n \equiv 0 \mod 4$ condition,

$$f_E(q,n) = 2\binom{n}{2q} < 2\binom{n}{n/2} = 2\binom{n}{2n/4} = f_E(n/4,n).$$

Corollary 11 *The sum of all possible* $\{f_E(q,n)\}_{0\le q\le\lfloor\frac{n}{2}\rfloor}$ *is equal to* $f_\Omega(n)$,

$$\sum_{q=0}^{\lfloor\frac{n}{2}\rfloor} f_E(q,n) = f_\Omega(n) = 2^n. \tag{29}$$

Proof Collecting all possible numbers, we have the following equations:

$$\begin{aligned}
\sum_{q=0}^{\lfloor\frac{n}{2}\rfloor} f_E(q,n) &= \sum_{q=0}^{\lfloor\frac{n}{2}\rfloor} 2\binom{n}{2q} \\
&= 2\sum_{q=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2q}, \quad \sum_{k\ge 0}\binom{n}{2k} = \sum_{k\ge 0}\binom{n}{2k+1} = 2^{n-1} \\
&= 2\times 2^{n-1} \\
&= 2^n \\
&= f_\Omega(n).
\end{aligned}$$

3.4 Relationships of Four Symmetric Clusters

Theorem 4 *For any* $n > 0$, *the sum of all possible functions on* $\{f(q,p,n\}_{\forall p,\forall q}$ *or* $\{f_E(q,n)\}_{0\le q\le\lfloor\frac{n}{2}\rfloor}$ *or* $\{f_L(p,n)\}_{p=0}^{n}$ *or* $\{f_G(m,n)\}$, $1 \le m \le C_G(n)$ *is equal to* $f_\Omega(n)$

$$\begin{aligned}
f_\Omega(n) &= \sum_{\forall p}\sum_{\forall q} f(q,p,n) = \sum_{q=0}^{\lfloor\frac{n}{2}\rfloor} f_E(q,n) = \sum_{p=0}^{n} f_L(p,n) \\
&= \sum_{m=1}^{C_G(n)} f_G(m,n) \\
&= 2^n.
\end{aligned} \tag{30}$$

Proof From the results of Corollaries 4, 8 and 11, four schemes provide various partitions to the same set of vectors on $\Omega(n)$ completely.

Corollary 12 *Numbers of four symmetric clusters can be expressed by*

Table 8 Numbers of four symmetric clusters in $1 \leq n \leq 16$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$C_E(n)$	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9
$C_L(n)$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$C_V(n)$	2	3	4	6	8	11	14	18	22	27	32	38	44	51	58	66
$C_G(n)$	2	3	4	6	8	14	20	36	60	108	188	352	632	1182	2192	4116

$$
\begin{aligned}
C_E(n) &= \lfloor \frac{n}{2} \rfloor + 1; \\
C_L(n) &= n + 1; \\
C_V(n) &= \begin{cases} n^2/4 + 2, & n \equiv 0 \ mod\ 2 \\ (n^2 - 1)/4 + 2, & n \equiv 1 \ mod\ 2 \end{cases}; \\
C_G(n) &= \frac{1}{n} \sum_{k|n} \phi(k) 2^{\frac{n}{k}}.
\end{aligned}
$$

Proof Due to Lemmas 4, 6, 8 and Theorem 1, four equations for numbers of various symmetric clusters are listed.

In convenient for comparison, their values on $1 \leq n \leq 16$ are listed in Table 8, respectively.

Checking real clusters in four schemes, the following corollaries can be provided.

Corollary 13 *When $n = \{1, 2, 3\}$, three cluster schemes $C_L(n), C_V(n), C_G(n)$ provide the same partitions of clusters.*

Proof Checking the three schemes, we have $C_L(1) = C_V(1) = C_G(1) = 2, C_L(2) = C_V(2) = C_G(2) = 3$, $C_L(3) = C_V(3) = C_G(3) = 4$. Relevant cluster contains the same set of vectors.

Corollary 14 *When $n = \{1, 2, 3, 4, 5\}$, two cluster schemes $C_V(n), C_G(n)$ provide the same partitions of clusters.*

Proof Due to Corollary 13, we need to check $n = \{4, 5\}$ cases. For the two schemes, we have $(C_L(4) = 5) \neq (C_V(4) = C_G(4) = 6), (C_L(5) = 6) \neq (C_V(5) = C_G(5) = 8)$. Relevant cluster contains the same set of vectors.

Corollary 15 *When $n \geq 6$, four cluster schemes $C_E(n), C_L(n), C_V(n), C_G(n)$ provide different partitions on their clusters.*

Proof Due to Corollaries 13 and 14, we need to check $n = \{6, \cdots\}$ cases. For the four schemes, $C_E(6) = 4, C_L(6) = 7, C_V(6) = 11, C_G(6) = 14$. Only a few clusters can contain the same set of vectors.

Corollary 16 *When $n \geq 6$, three cluster schemes: combinatorial, crossing and variant $\{C_E(n), C_L(n), C_V(n)\}$ may contain more symmetric properties than rotation clusters on $C_G(n)$.*

Proof Considering a special case on $\{n = 6, p = 3, q = 2\}$, $V(2, 3, 6) = \{001101, 011010, 110100, 101001, 010011, 100110, 011001, 110010, 100101, 001011, 010110, 101100\}$; this cluster contains two cycles: {001101, 011010, 110100, 101001, 010011, 100110} and {011001, 110010, 100101, 001011, 010110, 101100} with six vectors, respectively. Both cycles have rotation symmetries only without reflection symmetries. It is possible to use reflection symmetric operators to distinct two relative cycles to form a pure rotation symmetric structure. However, other clusters may contain more cycles such as $L(3, 6)$ with four cycles and $E(2, 6)$ with six cycles, respectively. It is necessary to apply other symmetric operators different from rotation for further separations.

4 Four Number Sets of Symmetric Clusters

4.1 Four Approximates on Numbers of Clusters

Using the four numeric equations, relevant approximates can be expressed as follows.

Lemma 13 *Four approximates can be expressed as*

$$C_E(n) \approx O\left(\frac{n}{2}\right); \tag{31}$$

$$C_L(n) \approx O(n); \tag{32}$$

$$C_V(n) \approx O\left(\frac{n^2}{4}\right); \tag{33}$$

$$C_G(n) \approx O\left(\frac{2^n}{n}\right). \tag{34}$$

Proof Using the four equations, the following approximates can be expressed:

$$C_E(n) = \lfloor \frac{n}{2} \rfloor + 1 \approx O\left(\frac{n}{2}\right);$$

$$C_L(n) = n + 1 \approx O(n);$$

$$C_V(n) = \begin{cases} n^2/4 + 2, & n \equiv 0 \bmod 2 \\ (n^2 - 1)/4 + 2, & n \equiv 1 \bmod 2 \end{cases} \approx O\left(\frac{n^2}{4}\right);$$

$$C_G(n) = \frac{1}{n} \sum_{k|n} \phi(k) 2^{\frac{n}{k}} \approx O\left(\frac{2^n}{n}\right).$$

4.2 Four Approximates on Numbers of Vectors

Definition 22 Let $f_X(n)$, $X \in \{L, E, V, G\}$ denote an approximate number of vectors in X cluster.

Lemma 14 *Four approximates can be expressed as*

$$f_E(n) \approx O\left(\frac{2^{n+1}}{n}\right); \tag{35}$$

$$f_L(n) \approx O\left(\frac{2^n}{n}\right); \tag{36}$$

$$f_V(n) \approx O\left(\frac{2^{n+2}}{n^2}\right); \tag{37}$$

$$f_G(n) \approx O(n). \tag{38}$$

Proof Since all clusters partition the same phase space $\Omega(n)$ with 2^n vectors, their approximates for vectors in a cluster can be evaluated,

$$f_E(n) = \frac{2^n}{O\left(\frac{n}{2}\right)} \approx O\left(\frac{2^{n+1}}{n}\right);$$

$$f_L(n) = \frac{2^n}{O(n)} \approx O\left(\frac{2^n}{n}\right);$$

$$f_V(n) = \frac{2^n}{O\left(\frac{n^2}{4}\right)} \approx O\left(\frac{2^{n+2}}{n^2}\right);$$

$$f_G(n) = \frac{2^n}{O\left(\frac{2^n}{n}\right)} \approx O(n).$$

It is convenient to list approximate numbers on clusters, vectors and dimension of measuring phase spaces in Table 9.

Table 9 Four approximate numbers on both clusters and vectors

X	$C_X(n)$	$f_X(n)$	Measuring phase space
E	$O\left(\frac{n}{2}\right)$	$O\left(\frac{2^{n+1}}{n}\right)$	1D
L	$O(n)$	$O\left(\frac{2^n}{n}\right)$	1D
V	$O\left(\frac{n^2}{4}\right)$	$O\left(\frac{2^{n+2}}{n^2}\right)$	2D
G	$O\left(\frac{2^n}{n}\right)$	$O(n)$	1D

5 Symmetric Boolean Functions for Selected Clusters

5.1 Four Numbers on Symmetric Boolean Functions

Definition 23 Let $SF_X(n)$ denote a number of Symmetric Boolean Functions (SBF) in $\{X(.)\}$, $X \in \{E, L, V, G\}$.

Theorem 5 (Four types of symmetric Boolean functions) *Total numbers of four types of symmetric Boolean functions* $SF_X(n)$, $X \in \{E, L, V, G\}$ *are*

$$SF_E(n) = 2^{C_E(n)} = 2^{\lfloor \frac{n}{2} \rfloor + 1}; \tag{39}$$

$$SF_L(n) = 2^{C_L(n)} = 2^{n+1}; \tag{40}$$

$$SF_V(n) = 2^{C_V(n)} = \begin{cases} 2^{n^2/4+2}, & n \equiv 0 \ mod\ 2 \\ 2^{(n^2-1)/4+2}, & n \equiv 1 \ mod\ 2 \end{cases}; \tag{41}$$

$$SF_G(n) = 2^{C_G(n)} = O\left(2^{\frac{2^n}{n}}\right). \tag{42}$$

Proof For any selected cluster, there are two selections for its symmetric Boolean functions.

5.2 Four Numbers of Balanced Symmetric Clusters

Definition 24 Let $SF_{Xb}(n)$ be a maximal number of balanced SBF_X in $\{X(.)\}$, $X \in \{L, V, G\}$, $n = 0 \bmod 2$.

Definition 25 Let $SF_{Eb}(n)$ be a maximal number of balanced SBF_E in $\exists q$, $\{E(q, n)\}$, $n = 0 \bmod 4$.

Lemma 15 *Four selected numbers* $\{C_{Xb}(n)\}$, $X \in \{E, L, V, G\}$ *for balanced symmetric clusters are*

$$C_{Eb}(n) = \begin{cases} 1, & n \equiv 0 \mod 4 \\ 0, & n \neq 0 \mod 4 \end{cases}; \tag{43}$$

$$C_{Lb}(n) = 1; \tag{44}$$

$$C_{Vb}(n) = \frac{n}{2}; \tag{45}$$

$$C_{Gb}(n) = O\left(\frac{1}{n}\binom{n}{n/2}\right). \tag{46}$$

Proof From Corollary 10 for Eb groups $n \equiv 0 \mod 4$ cases, $q = n/4$ provides a cluster with a maximal number of vectors in a balanced condition and other cases cannot satisfy balanced conditions; for Lb groups $n \equiv 0 \mod 2$ cases, $p = n/2$

Table 10 Numbers of four balanced symmetric functions in $2 \le n \le 20$

n	2	4	6	8	10	12	14	16	18	20
$2^{C_{Eb}(n)}$	1	2	1	2	1	2	1	2	1	2
$2^{C_{Lb}(n)}$	2	2	2	2	2	2	2	2	2	2
$2^{C_{Vb}(n)}$	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
$2^{C_{Gb}(n)}$	2^1	2^2	2^4	2^{10}	$O\left(2^{25.2}\right)$	$O\left(2^{77}\right)$	$O\left(2^{245.1}\right)$	$O\left(2^{804.3}\right)$	$O\left(2^{2701.1}\right)$	$O\left(2^{9237.8}\right)$

provides a cluster with a maximal number of vectors in a balanced condition; for Vb groups $n \equiv 0 \mod 2$ cases, $p = n/2$, $1 \le q \le n/2$, there are $n/2$ clusters involved in a balanced condition; for Gb groups $n \equiv 0 \mod 2$ cases, $p = n/2$, a total of rotation symmetric clusters $O\left(\frac{1}{n}\binom{n}{n/2}\right)$ could be involved in a balanced condition.

5.3 Four Numbers of Balanced Symmetric Boolean Functions

Theorem 6 (Four balanced SYMMETRIC Boolean functions) *Total numbers of four balanced symmetric Boolean functions* $\{SF_Xb(n)\}$, $X \in \{E, L, V, G\}$ *are*

$$SF_{Eb}(n) = 2^{C_{Eb}(n)} = \begin{cases} 2, & n \equiv 0 \mod 4 \\ 1, & n \neq 0 \mod 4 \end{cases}; \tag{47}$$

$$SF_Lb(n) = 2^{C_{Lb}(n)} = 2; \tag{48}$$

$$SF_Vb(n) = 2^{C_{Vb}(n)} = 2^{\frac{n}{2}}; \tag{49}$$

$$SF_Gb(n) = 2^{C_{Gb}(n)} = O\left(2^{\frac{1}{n}\binom{n}{n/2}}\right). \tag{50}$$

Proof Each number of clusters in a selected scheme has been determined in Lemma 15. For any selected cluster in the scheme, there are two selections to form relevant symmetric Boolean functions.

In convenient for comparison, four types of SBF_{Xb} numbers on $2 \le n \le 20$ are listed in Table 10, respectively.

6 Cryptographic Properties of Symmetric Boolean Functions in Hierarchy

Boolean functions are of great importance in the design of random number generators for stream ciphers [25] that are widely used in modern network environment.

Due to cryptographically secure consideration, the sequence produced by the random number generator must satisfy the various properties [6, 8]: the longer period, the period complexity and good statistical distributions. There exists a huge theoretical knowledge of such combining generators [25].

A symmetric Boolean function must fulfil different necessary criteria to yield a cryptographically secure scheme, at least to resist known attacks [11]. In this direction, various measuring parameters play an important role such as balanced, support set, hamming weight, hamming distance, balanced function, non-linearity, correlation immunity, etc. [6, 8].

In relation to balanced properties, when n is even, the functions of highest non-linearity are the bent functions, and it is well known that the bent functions cannot be the balanced functions [28, 33]. From a structural viewpoint, the balanced functions having the highest possible non-linearity need to be considered. However, finding such functions is a very difficult problem [29, 31, 33]. When n is odd, exhibiting functions of the highest non-linearity is a hard problem in itself. Among the available candidates, balanced ones exist [16, 33].

To explore optimal functions in rotation symmetric Boolean function sets, many researchers are faced extremely difficulties on computational complexity even for $n > 10$ symmetric Boolean functions [29]. Exponentially increasing complexity makes a complex exhaustive search be quickly impossible. Compared with both variant and rotation schemes listed in Table 10, it is interesting to notice that the variant scheme takes a numeric complexity on $n = 20$ as same as the rotation symmetric scheme on $n = 10$. Much faster computation on optimal functions could be feasibly explored.

From a meta analytic viewpoint, measuring phase spaces provide multiple levels of construction in a hierarchy linked to various symmetric Boolean functions. They support an n tuple 0–1 vector construction as a word-based 0–1 vector to satisfy various design and analysis purposes. The variant PRNG construction [38, 43] is a similar approach to RC4 and HC128 stream ciphers [25] in their meta phase spaces using the word-oriented vector structure with the higher speed and efficiency. Measuring phase spaces could support advanced cryptographic applications on the direction.

Due to significant differences between measuring phase spaces proposed and algebraic normal forms classically formulated, in addition to initial balanced symmetric properties discussed in the chapter, other advanced comparison mechanisms need to be established for all interesting cryptographic properties to satisfy practical and optimal requirements for stream ciphers. Further detailed researches and explorations are required.

7 Conclusion

Symmetric clusters in a hierarchy provide the additional information to organize various symmetric Boolean functions into hierarchical constructions as multiple meta

levels of structures efficiently. The variant symmetric functions proposed in this chapter provide a meta construction on a 2D measuring phase space to contribute richer capacities compared with the three classical schemes (combinatorial, crossing and rotation) on 1D measuring phase spaces.

From a measuring viewpoint, three schemes (combinatorial, variant and rotation) in Tables 8, 9 and 10 have similar values in $n = \{1, 2, 3\}$ and $\{4, 5\}$ or different values in $n \geq 6$ conditions. The variant scheme provides a 2D intermediate structure different from other two schemes in 1D structure. From an approximate viewpoint, both combinatorial and rotation schemes are shown in stronger similar properties. Their approximate number of clusters and number of vectors in a cluster can be exchanged in Table 9. From an abstract system viewpoint, this pair of exchangeable measurements may provide approximate symmetric properties for both combinatorial and rotation schemes.

From a clustering viewpoint, the most important results are summarized in Theorem 4 to show that the four symmetric cluster schemes are different partition schemes on the same 0–1 vector set.

From a balanced analysis viewpoint, the key results of balanced symmetric Boolean functions are summarized in Theorem 6 and Table 10. This set of results provides a basic measurement to illustrate relevant computational difficulties to explore further optimal properties in balanced symmetric conditions. Different from other three schemes (combinatorial, crossing and rotation) in either very simpler or extremely complex associated with n increasing, balanced variant symmetric Boolean functions present very interesting patterns to support even $n \geq 20$ cases for future explorations.

Many advanced properties are existed to use a meta hierarchical construction to manage relevant measuring phase spaces into multilevels of a hierarchical structure. Various measuring parameters can be used as control parameters in detailed cases. Refined design and analysis can be performed under this meta hierarchy to provide powerful models and tools on design and optimization for future generations of stream ciphers.

References

1. E.B. Barker, A Statistical test suite for random and pseudorandom number generators for cryptographic applications, ITLB NIST (2000)
2. J.V. Bradley, *Distribution-free statistical tests* (Prentice-Hall 1968)
3. J. Carroll, The binary derivative test: noise filter, crypto aid, and random-number seed selector. Simulation **53**(3), 129–135 (1989)
4. P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms* (Cambridge University Press, Cambridge, 1994)
5. A. Canteaut, M. Videau, Symmetric boolean functions. IEEE Trans. Inf. Theory **51**(8), 2791–2811 (2005)
6. C. Carlet, On the degree, nonlinearity, algebraic thickness and nonormality of boolean function, with developments on symmetric functions. IEEE Trans. Inf. Theory **50**(9), 2178–2185 (2004)

7. C. Carlet, K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity for fast algebraic attacks and good nonlinearity, in *ASIACRYPT* ed. by J. Pieprzyk, LNCS, vol. 5350 (Springer 2008), pp. 425–440
8. C. Carlet, G. Gao, W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. *J. Comb. Theory*, Ser. A, **127**, 161–175 (2014)
9. F.N. Castro, L.A. Medina, Linear recurrences and asymptotic behavior of exponential sums of symmetric boolean functions. Electron. J. Combin. **18**(2), P8 (2011)
10. J.R. Chen. *Combinatorial Mathematics* (Harbin Institute of Technology Press, 2012) (in Chinese)
11. T.W. Cusick, P. Stănică. Fast Evaluation, weights and nonlinearity of rotation-symmetric functions. Discrete Mathe. **258**(1-3), 289–301 (2002)
12. E. Filiol, C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation immunity, in *Eurocrypt 1998*, number 1403 in Lecture Notes in Computer Science, vol. 475488 (Springer-Verlag, 1998)
13. S.J. Fu, C. Li, L.J. Qu, On the number of rotation symmetric boolean functions. Sci. China Inf. Sci. **53**(3), 537–545 (2010)
14. H.W. Gould, Some generalizations of vandermonde's convolution. Am. Math. Mon. **63**(2), 84–91 (1956)
15. H.W. Gould. *Combinatorial Identities* (Morganton, 1972)
16. Y.M. Guo, G.P. Gao, Y.Q. Zhao. Recent results on balanced symmetric boolean functions, available: http://eprint.iacr.org/2012/093 (2012)
17. G. Gao, X. Zhang, W. Liu, C. Carlet, Constructions of quadratic and cubic rotation symmetric bent functions. IEEE Trans. Inf. Theory **58**(7), 4908–4913 (2012)
18. M. Hall, *Combinatorial Theory*, 2nd edn. (Blaisdell, 1986)
19. L.K. Hua,*Loo-Keng Hua Selected Papers* (Springer, 1982)
20. S. Kavut, S. Maitra, M.D. Ycel, Search for boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inf. Theory **53**(5), 1743–1751 (2007)
21. D.E. Knuth. *The Art of Computer Programming*, vol. 1, 3rd edn. (Addison-Wesley, 1998)
22. D.E. Knuth, *The Art of Computer Programming, A: Combinatorial Algorithms*, Part 1, vol. 4 (Addison-Wesley, 2011)
23. B. Logan Jr., Information in the zero crossings of bandpass signals. Bell Syst. Tech. J. **56**, 487–510 (1977)
24. Q. Meng, L. Chen, F. Fu, On homogeneous rotation symmetric bent functions. Discr. Appl. Math. **158**(10), 1111–1117 (2010)
25. G. Paul, S. Maitra. *RC4 Stream Cipher and Its Variants* (CRC Press, 2012)
26. J. Pieprzyk, C.X. Qu, Fast hashing and rotation-symmetric functions. J. Universal Comput. Sci. **5**(1), 20–31 (1999)
27. L. Qu, C. Li, K. Feng, A note on symmetric boolean functions with maximum algebraic immunity in odd number of variables. IEEE Trans. IT-53, 2908–2910 (2007)
28. Sarkar, P., Maitra, S, Construction of nonlinear Boolean functions with important cryptographic properties, in *Advances in Cryptology EUROCRYPT 2000*, vol. 1807 in LNCS (Springer Verlag, 2000), pp. 485–506
29. P. Stănică, S. Maitra, Rotation symmetric boolean functions - count and cryptographic properties, Discr. Appl. Math. **156**, 1567–1580 (2008)
30. R.P. Stanley, *Enumerative Combinatorics*, Vol. 1, 2nd edn. (Cambridge University Press, 1997)
31. W. Su, X.H. Tang, A. Pott, A note on a conjecture for balanced elementary symmetric boolean functions. IEEE Trans. Inf. Theory **59**(1), 665–671 (2013)
32. S.H. Su, X.H. Tang, Construction of rotation symmetric boolean functions with optimal algebraic immunity and high nonlinearity. Des. Codes Cryptography **71**(2), 183–199 (2014)
33. S.H. Su, X.H. Tang, On the systematic constructions of rotation symmetric bent functions with any possible algebraic degrees. IACR Cryptology ePrint Archive **2015**, 451 (2015)
34. G.Z. Tu, *Combinatorial Enumeration Methods & Applications* (Science Press, 1981) (in Chinese)

35. A. Tucker, *Applied Combinatorics* (Wiley, 2007)
36. J.H. van Lint, R.M. Wilson, *A Course in Combinatorics*, 2nd edn. (Cambridge University Press, 2001)
37. H. Wang, J. Zheng, 3D Visual Method of Variant Logic Construction for Random Sequence. Australian Information Warfare and Security, pp. 16–27 (2013)
38. W.Z. Yang, J. Zheng, Variant pseudo-random number generator, Hakin9 extra. Timing Attack **06**(13), 28–31 (2012)
39. Z.J. Zheng, A. Maeder, The conjugate classification of the kernel form of the hexagonal grid, in *Modern Geometric Computing for Visualization* (Springer-Verlag, 1992) pp. 73–89. http://link.springer.com/chapter/10.1007/978-4-431-68207-3_5 e-version
40. Z.J. Zheng. *Conjugate Transformation of Regular Plan Lattices for Binary Images*, Ph.D. Thesis, Monash University, 1994
41. J.Z.J. Zheng, C.H.H. Zheng, A framework to express variant and invariant functional spaces for binary logic, *Frontiers of Electrical and Electronic Engineering in China*, **5**(2), 163–172, Higher Educational Press and Springer-Verlag, 2010. http://link.springer.com/article/10.1007%2Fs11460-010-0011-4, https://doi.org/10.1007/s11460-010-0011-4
42. J.Z.J. Zheng, C.H.H. Zheng, T.L. Kunii, A framework of variant logic construction for cellular automata, *Cellular Automata - Innovative Modeling for Science and Engineering*, ed by A. Salcido (InTech Press, 2011). http://www.intechopen.com/books/cellular-automata-innovative-modelling-for-science-and-engineering/a-framework-of-variant-logic-construction-for-cellular-automata, https://doi.org/10.5772/15400
43. J. Zheng, Novel pseudo-random number generation using variant logic framework, in *2nd International Cyber Resilience Conference*, pp. 100–104, 2011. http://igneous.scis.ecu.edu.au/proceedings/2011/icr/zheng.pdf
44. J. Zheng, C. Zheng, Variant simulation system using quaternion structure. J. Modern Opt. Taylor & Francis Press **59**(5), 484–492 (2012)
45. J. Zheng, C. Zheng, T.L. Kunii, From conditional probability measurements to global matrix representations on variant construction, in *Advanced Topics in Measurements* (InTech Press, 2012), pp. 339–370
46. J. Zheng, C. Zheng, T.L. Kunii. From Local Interactive Measurements to Global Matrix Representations on Variant Construction, in *Advanced Topics in Measurements* (InTech Press, 2012), pp. 371–400
47. J. Zheng, C. Zheng, T.L. Kunii, Interactive maps on variant phase space, in *Emerging Application of Cellular Automata* (InTech Press, 2013), pp. 113–196
48. J. Zheng, W. Zhang, J. Luo, W. Zhou, R. Shen, Variant map system to simulate complex properties of DNA interactions using binary sequences. Adv. Pure Math. **3**(7A), 5–24 (2013)
49. J. Zheng, J. Luo, W. Zhou, Pseudo DNA sequence generation of non-coding distributions using variant maps on cellular automata. Appl. Math. **5**(1), 153–174 (2014)
50. J. Zheng, W. Zhang, J. Luo, W. Zhou, V. Liesaputra, Variant map construction to detect symmetric properties of genomes on 2D distributions. J. Data Mining Genomics Proteomics **5**, 150 (2014). https://doi.org/10.4172/2153-0602.1000150