New (ideas) Invariants for Boolean and Vectorial Functions

Valérie Gillot – Philippe Langevin

BFA 2026 Sogndal (Norway)

IMATH – Université de Toulon

Presentation

Within the framework of the SWAP project[1], we have established several results on 6-bit APN mappings : two-level spectral functions, closure under switchings, APN extension of (6,3)-bent...

Gillot and Langevin 2026, *On Known APNs*

In this talk, I focus on invariants that we used to obtain these results.

[1] https://anr.fr/Projet-ANR-21-CE39-0012

Almost Perfect Nonlinear mapping

A mapping $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is APN [2-flat breaker]

$$x + y + z + t = 0 \quad \text{(all distinct)} \qquad \Longrightarrow \qquad F(x) + F(y) + F(z) + F(t) \neq 0$$

In the case $m = 6$, it is widely conjectured that all 6-bit APN mappings are known :

- 716 EA-classes.
- $14 = 13 + 1$ CCZ-classes.

Challenge: Construct efficient invariants to distinguish these classes.

Calderini 2020, *On the EA-classes of known APN functions in small dimensions*

exploration of 2-switchs of known apn mappings

$F, G : \mathbb{F}_2^m \to \mathbb{F}_2^m$

$$\textsc{comp}(F) := \{\, b \cdot F \;:\; b \in \mathbb{F}_2^m \,\}, \qquad \textsc{comp}(G) := \{\, b \cdot G \;:\; b \in \mathbb{F}_2^m \,\}$$

One says that G is a *k-switch* of F if

$$\dim\big(\textsc{comp}(F) \cap \textsc{comp}(G)\big) = m - k.$$

Edel–Pott A new APN via 1-switch, CCZ-inequivalent to any quadratic function.

Edel and Pott 2009, *A new almost perfect nonlinear function which is not quadratic*

Fact
The set of known APN is closed under 1-switch

Closure under 2-switches

We say that $F : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^k$ is a (m, k)-subfunction of G when

$$\textsc{comp}(F) \subseteq \textsc{comp}(G).$$

In that case, G is an extension of F.

Starting from a set of representative of 716 known APN classes

1. **enumerate** all the (6,4)-subfunctions.
2. **filter** using a vectorial invariant
3. **extend** survival candidates into APN extension by backtracking
4. **reduce** to EA-equivalence

a search for new APN *mappings among the* **2-switches** *of known ones*

Invariant and Equivalence

$G, F\colon \mathbb{F}_2^m \to \mathbb{F}_2^n$ are *r-equivalent* if

$$G = B \circ F \circ A \quad \text{up to degree } r,$$

for some affine permutations A, B.

- The case $r < 0$ is affine equivalence.
- The case $r = 1$ is EA-equivalence.

An *invariant* $\jmath$ satisfies

$$G \underset{r}{\sim} F \Longrightarrow \jmath(G) = \jmath(F).$$

A *collision* is a pair $G \underset{r}{\not\sim} F$ with $\jmath(G) = \jmath(F)$.

Boolean functions

Every $f \in \mathrm{B}(m)$ has a unique ANF

$$f(x) = \sum_{S \subseteq \{1,\dots,m\}} a_S X_S, \qquad \deg(f) = \max\{|S| : a_S = 1\}, \quad \mathrm{val}\,(f) = \min\{|S| : a_S = 1\}.$$

usual spaces :

$$\mathrm{RM}(p,m) = \{f \mid \deg(f) \leq p\} \qquad \mathrm{B}_s^t(m) = \{f \mid \mathrm{val}\,(f) \geq s,\ \deg(f) \leq t\}$$

Basic invariants : degree, and the *absolute Walsh spectrum*

$$f \mapsto \mathrm{walsh}(f) = \{\{\ |\widehat{f}(a)|\ :\ a \in \mathbb{F}_2^m\ \}\}$$

$\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+ax}$

From class number to classification

The number of classes is **easy** to compute using Burnside's formula — identifying a set of representatives may be **hard**!

$$\tilde{\mathrm{B}}_s^t(m) := \text{a set of representatives of } \mathrm{B}_s^t(m)$$

$\tilde{\mathrm{B}}_1^5(5)$	$\tilde{\mathrm{B}}_2^6(6)$	$\tilde{\mathrm{B}}_3^3(8)$	$\tilde{\mathrm{B}}_3^3(9)$	$\tilde{\mathrm{B}}_4^4(8)$	$\tilde{\mathrm{B}}_3^4(7)$	$\tilde{\mathrm{B}}_3^3(10)$	$\tilde{\mathrm{B}}_3^4(8)$
206	150356	32	349	999	68443	3691561	$10^{16.7}$
1972	1991	1991	2003	2008	2023	2026	?
Berlekamp	Maiorana	Hou	Brier	Leander	Gillot	Khoruzhii	?

Brier and Langevin 2003, *The classification of boolean cubics of nine variables.*

Khoruzhii, Gelss, and Pokutta 2026, *Classification of Boolean Cubic Forms in Ten Variables*

Restriction to affine hyperplane

For $0 \neq u \in \mathbb{F}_2^m$:

$$H_u := \{x \in \mathbb{F}_2^m \mid ux = 0\}, \qquad \bar{H}_u := \{x \in \mathbb{F}_2^m \mid ux = 1\}.$$

Considering the restrictions of $f \in \mathrm{B}(m)$,

$$f\Big|_u \colon H_u \to \mathbb{F}_2 \qquad f\Big|_{\bar{u}} \colon \bar{H}_u \to \mathbb{F}_2$$

For any invariant $\jmath$ on $\mathrm{B}(m-1)$, we consider the (small) multiset :

$$R_f(u) := \{\{\ \jmath(f\big|_u),\ \jmath(f\big|_{\bar{u}}\ \}\}.$$

Lifting by restriction for Boolean function

$$
\begin{tikzcd}
 & \mathrm{B}_s^t(m+1) \arrow[r, dash, dashed, "\text{Fourier}"] \arrow[d, "\jmath'"] \arrow[ddl, dash, dashed, "\text{restriction}"'] & \mathrm{B}_s^t(m+1) \arrow[d, "\widehat{\jmath}"] \\
 & \cdots & \cdots \\
\mathrm{B}_s^t(m) \arrow[d, "\jmath"] & & \\
X & &
\end{tikzcd}
$$

$$f \mapsto \jmath'(f) := \{\!\{\ R_f(u) \mid 0 \neq u \in \mathbb{F}_2^m\ \}\!\}$$

Using Fourier-Hadamard transform:

$$f \mapsto \widehat{\jmath}(f) := \{\!\{\ \widehat{R_f(a)} \mid a \in \mathbb{F}_2^m\ \}\!\}$$

$\widehat{R_f(a)} = \sum_{0 \neq u \in \mathbb{F}_2^m} R_f(u)(-1)^{au}$

Very efficient on 6-bit functions!

There are $\sharp\tilde{\mathrm{B}}_2^5(5) = 48$ classes in dimension 5, and $\sharp\tilde{\mathrm{B}}_2^6(6) = 150\,356$ in dimension 6.
Lifting a class indicator $\omega\colon \mathrm{B}_2^5(5) \to \tilde{\mathrm{B}}_2^5(5)$ by restriction gives :

	ω'	$\widehat{\omega}$
$\sharp$-value	150338	150355
$\sharp$-collision	18	1

Only one collision on 150 356 classes:

$$ab + bc + cd + bce + abde + abcf + adf \quad \text{vs.} \quad ac + bc + bd + bce + abde + abcf + adf$$

Computing this invariant on all classes takes 18 seconds.

Gillot and Langevin 2022, *Classification of* $\mathrm{B}_s^t(m)$

Observation of components of known APN

The 716 classes of known 6-bit APN functions have algebraic degrees 2, 3, or 4.

Observing the EA-class of all their components ($716 * 63 = 45108$):

Fact
The set of components of known 6-bit APN *reduces to* **37** EA*-classes !*

Problem
How to decide if a given Boolean function is a component of some APN mapping?

Conjecture
If F is an APN *mapping then* $\deg(F) < m$

Lifting by composition for vectorial functions

Let $\jmath$ be an invariant on $\mathrm{B}_s^t(m)$. It lifts by composition to an invariant on $V_s^t(m,n)$:

$$\jmath_c(F) := \{\!\{\jmath(f) \mid f \in \textsc{comp}(F)\}\!\}$$

Lifting by restriction works here too:

$$\begin{tikzcd} & & V_s^t(m+1,n) \\ & V_s^t(m,n) \arrow[ur, dash, dashed, "\widehat{\jmath_c}", "\text{restriction}"'] & \\ \jmath\colon \mathrm{B}_s^t(m) \arrow[ur, dash, dashed, "\jmath_c", "\text{composition}"'] & & \end{tikzcd}$$

baby example : (4,4)-vectorial mapping

$$\sharp \mathrm{V}(4,4) = (2^{2^4})^4 = 2^{64} \approx 10^{19} \quad \Longrightarrow \quad 4\,713 \text{ EA-classes (Brinkmann, 2019)}$$

$$\begin{tikzcd}
 & & \mathrm{V}(4,4) & \\
 & \mathrm{V}(3,4) \arrow[ur, dashed, "\widehat{\omega_{3c}}\ \textit{(restriction)}"] & & \\
\omega_3 \colon \mathrm{B}_2^3(3) \to \tilde{\mathrm{B}}_2^3(3) \arrow[ur, "\omega_{3c}\ \textit{(composition)}"] & & & \omega_4 \colon \mathrm{B}_2^4(4) \to \tilde{\mathrm{B}}_2^4(4) \arrow[uul, "\omega_{4c}\ \textit{(composition)}"']
\end{tikzcd}$$

Invariant	walsh	ω_{4c}	$\widehat{\omega_{3c}}$
$\sharp$-values	481	951	3828
Combination		4458	

Lifting to $V_2^6(6,6)$

$$
\begin{tikzcd}
 & & V_2^6(6,6) & \\
 & V_2^5(5,6) \arrow[ur, dashed, "\widehat{\omega_c}"] & & \mathrm{B}_2^6(6) \arrow[ul, dashed, "\hat{\omega}_c"'] \\
\omega : \mathrm{B}_2^5(5) \to \tilde{\mathrm{B}}_2^5(5) \arrow[ur, dashed, "\omega_c"] \arrow[urrr, dashed, "\hat{\omega}"'] & & &
\end{tikzcd}
$$

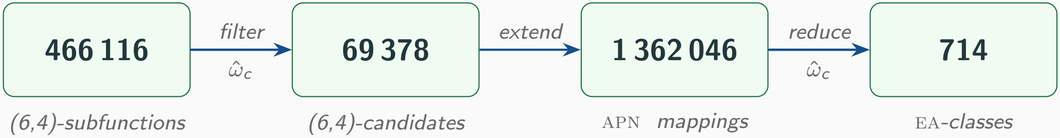
Effectiveness of theses lifts

The Fourier lift $\hat{\omega}_c$ takes **714** values on the set of known APN , and providing **only two** collisions (among quadratic functions).

Invariant	DDT	LAT	ZT	$\widehat{\omega_c}$	$\hat{\omega}_c$
$\sharp$-values	2	2	41	157	714

Remark
$\hat{\omega}_c$ looks like a very good choice for 2-switching analysis.

Numerical result



Starting from the 716 known EA-classes of 6-bit APN functions, the pipeline enumerates their (6,4)-subfunctions and filters them with the vectorial invariant $\hat{\omega}_c$.

Surviving candidates are then extended into APN mappings by backtracking, and reduced to affine equivalence.

The set of known apn appears to be closed under 2-switchings

2-switching of known 6-bit APNs

14 CCZ classes of known APN														
num	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ea	25	19	91	19	3	13	91	3	92	85	85	91	13	86
sub	16275	12369	59241	12369	1953	8463	59241	1953	59892	55335	55335	59241	8463	55986
filter	5945	2133	8263	1699	193	1111	8493	65	8315	8188	7878	8170	1584	7341
apns	41626	85271	154303	63682	6069	34076	154832	2928	156167	154780	147546	161340	55048	144378
classe	519	700	704	694	473	701	704	353	706	703	704	704	688	706

For the details :

Gillot and Langevin 2026, *Observation of known APNs*

ccz-equivalence

Considering the *graph* of $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$

$$\Gamma(F) = \{(x, F(x)) \mid x \in \mathbb{F}_2^m\} \subseteq \mathbb{F}_2^{m+n} \rightsquigarrow \mathrm{B}(m+n).$$

One defines

$$\Gamma(F) \sim \Gamma(G) \iff F \underset{\text{CCZ}}{\sim} G$$

Problem
Design efficient invariants to discriminate the 14 CCZ-classes of 6-bit known APN .

Kaleyski pointed out that the combination of Γ-rank and Δ-rank takes 10 values.

CCZ-invariant	walsh	Γ-rank	Δ-rank
time	0.01s	1.06s	0.80s
♯-values	2	9	3
combination	11		

Kaleyski 2021, *Invariants for EA-and CCZ-equivalence of APN and AB functions*

multiplicative invariant

Choosing a parameter $0 \leq p \leq m$,

For a Boolean function $f \in \mathrm{B}(m)$,

$$\begin{aligned} \mathsf{X}_p^f\colon \mathrm{RM}(p,m) &\longrightarrow \mathrm{B}(m) \\ c &\longmapsto c \times f \end{aligned}$$

The dimension of the kernel of is a numerical invariant $\mathsf{X}_p(f) := \dim\ker \mathsf{X}_p^f$.

CCZ-invariant	X_1	X_2	X_3
time	0.01s	0.04s	0.15s
$\sharp$-values	2	7	2
combination	7		

Multiplicative invariants on graph of 6-bit APN .

Walsh refinement

Denote by ν_2 the 2-adic valuation on integers, $\nu_2(z) := \max\{r \in \mathbb{N} \mid 2^r \text{ divides } z\}$.

For $f \in \mathrm{B}(m)$,

$$\nu_2\big(\widehat{f}(a)\big) \in \{\infty, 0, 1, \ldots, m\}$$

For each v, we define $\psi_v \in \mathrm{B}(m)$:

$$\psi_v(a) = 1 \iff \nu_2\big(\widehat{f}(a)\big) = v.$$

The *Walsh refinement* of f by $\jmath$ is the tuple

$$\mathrm{W}_\jmath(f) := \big(\jmath(\psi_\infty), \jmath(\psi_0), \ldots, \jmath(\psi_m)\big).$$

CCZ-invariant	W_{X_1}	W_{X_2}	W_{X_3}
time	0.03s	0.15s	0.55s
$\sharp$-values	2	5	8
combination	8		

Walsh refinement of multiplicative invariants

Effectiveness of ccz-invariants from Boolean invariants

A combination of these three invariants takes 13 values on the 14 known classes and the combination of all invariants provides 1 collision.

<table>
<tr><td>Boolean Invariant</td><td>X_2</td><td>W_{X_3}</td><td>Γ-rank</td><td>Δ-rank</td></tr>
<tr><td>Running time</td><td>0.03s</td><td>0.55s</td><td>1.06s</td><td>0.80s</td></tr>
<tr><td>$\sharp$-values</td><td>7</td><td>8</td><td>9</td><td>3</td></tr>
<tr><td>Combination</td><td colspan="2">10</td><td colspan="2">10</td></tr>
<tr><td></td><td colspan="3">13</td><td></td></tr>
</table>

Problem
How to complete the list of invariant ?

(6,3)-bent function

An (m,n)-function F is bent if all its non-zero components are bent.

By Polujan's phd, we know there are 13 EA-classes of $(6,3)$-bent functions.

For a vectorial function $F \in \mathrm{V}(m,n)$,

$$\begin{array}{rcl} \bar{\mathsf{X}}_p^F : RM(p,m) & \longrightarrow & \mathrm{V}(m,n) \\ c & \longmapsto & \Pi_{p+1}(cF) \end{array}$$

Again, the dimension of the kernel is a vectorial EA-invariant denoted $\bar{\mathsf{X}}_3$.

Invariant	$\widehat{\omega_c}$	$\hat{\omega}_c$	$\bar{\mathsf{X}}_3$
$\sharp$-values	9	7	6
Combination		13	

Polujan 2021, *Boolean and vectorial functions : a design-theoretic point of view*

Conclusion

We introduced new methods for constructing effective Boolean and vectorial invariants: **lifting by restriction, by composition, multiplicative invariant and Walsh refinement**.

Several remarkable results

- on $B(2,6,6)$, only **one collision** among **150 356 classes**;
- for 6-bit APN mappings, **714 of the 716 classes** are distinguished;
- for $(6,3)$-bent functions, all **13 classes** are distinguished;
- three new Boolean invariants separate **13 of the 14 known ccz-classes**.

contributing to important numerical results

- all extensions of $(6,3)$-bent functions are known
- **closure under 2-switching** of the set of known APN

- Brier, Eric and Philippe Langevin (2003). **"The classification of boolean cubics of nine variables."**. In: *2003 IEEE Information Theory Workshop*. "La Sorbonne", Paris, France.
- Calderini, Marco (2020). **"On the EA-classes of known APN functions in small dimensions"**. English. In: *Cryptogr. Commun.* 12.5, pp. 821–840. ISSN: 1936-2447. DOI: 10.1007/s12095-020-00427-1.
- Edel, Yves and Alexander Pott (2009). **"A new almost perfect nonlinear function which is not quadratic"**. In: *Adv. Math. Commun.* 3.1, pp. 59–81. ISSN: 1930-5346,1930-5338. DOI: 10.3934/amc.2009.3.59. URL: https://doi.org/10.3934/amc.2009.3.59.

- Gillot, Valérie and Philippe Langevin (2022). **Classification of B(s, t, m).** http://langevin.univ-tln.fr/data/bst/.
- — (2026). **On Known APNs.** arXiv: 2601.11247 [cs.DM]. URL: https://arxiv.org/abs/2601.11247.
- Kaleyski, Nikolay (2021). **Invariants for EA- and CCZ-equivalence of APN and AB functions.** Cryptology ePrint Archive, Paper 2021/300. URL: https://eprint.iacr.org/2021/300.
- Khoruzhii, Kirill, Patrick Gelss, and Sebastian Pokutta (2026). **Classification of Boolean Cubic Forms in Ten Variables.** arXiv: 2606.28473 [math.NT]. URL: https://arxiv.org/abs/2606.28473.

Polujan, Alexander (2021). **"Boolean and vectorial functions : a design-theoretic point of view".** Available at http://dx.doi.org/10.25673/37956. PhD thesis. Otto-von-Guericke-Universität Magdeburg.

Comments

The number of class in $V_2^4(6,4)$ is about 10^{43}

weak point
The filtering step relies on $\hat{\omega}_c$ applied to $V_2^4(6,4)$. This invariant likely generates collisions.

running time
For backtracking, a few days using a lot of processors...

All refs i

- Berlekamp, Elwyn R. and Neil J. A. Sloane (1969). **“Restrictions on weight distribution of Reed-Muller codes”.** In: *Information and Control* 14, pp. 442–456.
- Berlekamp, Elwyn R. and Lloyd R. Welch (1972). **“Weight distributions of the cosets of the (32,6) Reed-Muller code”.** In: *IEEE Transactions on Information Theory* IT-18.1, pp. 203–207.
- Brier, Eric and Philippe Langevin (2003). **“The classification of Boolean cubics of nine variables”.** In: *Proceedings 2003 IEEE Information Theory Workshop*. Paris, France, pp. 179–182.
- Dickson, Leonard E. (1901). **Linear Groups, with an Exposition of the Galois Field Theory.** Reprinted, Dover Publications, 1958. Teubner.

All refs ii

- Dillon, John F. (1972). **A survey of bent functions.** Tech. rep. (rapport technique, diffusion restreinte).
- — (1974). **“Elementary Hadamard Difference Sets”.** PhD thesis. University of Maryland.
- Dougherty, Randall, R. Daniel Mauldin, and Mark Tiefenbruck (2022). **“The covering radius of the Reed-Muller code RM(m-4,m) in RM(m-3,m)”.** In: *IEEE Transactions on Information Theory* 68.1, pp. 560–571.
- Eliseev, V. A. and O. P. Stepchenkov (1962). **Rapports techniques non déclassifiés (fonctions “minimales”).** URSS ; référencés secondairement, ex. Mesnager, Carlet.
- Feulner, Thomas et al. (2013). **“Towards the classification of self-dual bent functions in eight variables”.** In: *Designs, Codes and Cryptography* 68, pp. 395–406.

All refs iii

- Gao, Jian et al. (2023). **The covering radius of the third-order Reed-Muller code RM(3,7) is 20.** Soumis à IEEE Transactions on Information Theory.
- Gillot, Valérie and Philippe Langevin (2022). **Classification of Boolean functions.** arXiv: 2208.02469.
- — (2023). **"Classification of some cosets of the Reed-Muller code".** In: *Cryptography and Communications* 15.6, pp. 1129–1137.
- — (2024). **"Coset leaders of the first-order Reed-Muller codes in four new classes of Boolean functions".** In: *Advances in Mathematics of Communications*.
- Gillot, Valérie, Philippe Langevin, and Alexandr Polujan (2024). **On the normality of Boolean quartics.** arXiv: 2407.14038.
- Golomb, Solomon W. (1959). **"On the classification of Boolean functions".** In: *IRE Transactions on Information Theory* 5.5, pp. 176–186.

- Hammons, A. Roger et al. (1994). **“The Z4-linearity of Kerdock, Preparata, Goethals, and related codes”.** In: *IEEE Transactions on Information Theory* 40.2, pp. 301–319.
- Harrison, Michael A. (1964). **“On the classification of Boolean functions by the general linear and affine groups”.** In: *Journal of the Society for Industrial and Applied Mathematics* 12.2, pp. 285–299.
- Hora, Jan and Petr Pudlák (2021). **“Classification of 9-dimensional trilinear alternating forms over GF(2)”.** In: *Finite Fields and Their Applications* 70, p. 101788.
- Hou, Xiang-Dong (1995). **“AGL(m,2) acting on R(r,m)/R(s,m)”.** In: *Journal of Algebra* 171.3, pp. 921–938.
- — (1996). **“GL(m,2) acting on R(r,m)/R(r-1,m)”.** In: *Discrete Mathematics* 149.1-3, pp. 99–122.

- Hou, Xiang-Dong (1998). **"Cubic bent functions".** In: *Discrete Mathematics* 189.1-3, pp. 149–161.
- Hou, Xiang-Dong and Philippe Langevin (1997). **"Results on bent functions".** In: *Journal of Combinatorial Theory, Series A* 80.2, pp. 232–246.
- Kasami, Tadao and Nobuki Tokura (1970). **"On the weight structure of Reed-Muller codes".** In: *IEEE Transactions on Information Theory* 16.6, pp. 752–759.
- Kavut, Selçuk and Subhamoy Maitra (2016). **"Patterson-Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound".** In: *IEEE Transactions on Information Theory* 62, pp. 2277–2282.
- Kavut, Selçuk, Subhamoy Maitra, and Melek D. Yücel (2007). **"Search for Boolean functions with excellent profiles in the rotation symmetric class".** In: *IEEE Transactions on Information Theory* 53, pp. 1743–1751.

- Kavut, Selçuk and Melek D. Yücel (2010). **"9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class"**. In: *Information and Computation* 208, pp. 341–350.
- Khoruzhii, Kirill, Patrick Gelss, and Sebastian Pokutta (2026). **Classification of Boolean Cubic Forms in Ten Variables.** arXiv: 2606.28473 [math.NT]. URL: https://arxiv.org/abs/2606.28473.
- Kurshan, R. P. and Neil J. A. Sloane (1972). **"Coset analysis of Reed-Muller codes via translates of finite vector spaces"**. In: *Information and Control* 20, pp. 410–414.
- Langevin, Philippe and Xiang-Dong Hou (2011). **"Counting partial spread functions in eight variables"**. In: *IEEE Transactions on Information Theory*.

- Langevin, Philippe and Gregor Leander (2008). **"Classification of the quartic forms of eight variables".** In: *Boolean Functions in Cryptology and Information Security*.
- — (2011). **"Counting all bent functions in dimension eight 99270589265934370305785861242880".** In: *Designs, Codes and Cryptography* 59.1-3, pp. 193–205.
- MacWilliams, Florence J. and Neil J. A. Sloane (1977). **The Theory of Error-Correcting Codes.** North-Holland.
- Maiorana, James A. (1991). **"A classification of the cosets of the Reed-Muller code R(1,6)".** In: *Mathematics of Computation* 57.195, pp. 403–414.

- Muller, David E. (1954). **"Application of Boolean algebra to switching circuit design and to error detection".** In: *IRE Transactions on Electronic Computers* EC-3, pp. 6–12.
- Nechiporuk, E. I. (1958). **"On the synthesis of networks using linear transformations of variables".** In: *Doklady Akademii Nauk SSSR* 123. English translation: Automation Express, April 1959, 12–13, pp. 610–612.
- Patterson, Nicholas J. and Douglas H. Wiedemann (1983). **"The covering radius of the (2^15,16) Reed-Muller code is at least 16276".** In: *IEEE Transactions on Information Theory* 29.3. Correction: IT-36(2), 1990, p. 443, pp. 354–356.
- Preneel, Bart (1993). **"Analysis and Design of Cryptographic Hash Functions".** PhD thesis. Katholieke Universiteit Leuven.

- Reed, Irving S. (1954). **"A class of multiple-error-correcting codes and the decoding scheme".** In: *IRE Transactions on Information Theory* 4, pp. 38–49.
- Rothaus, Oscar S. (1966). **On bent functions.** Tech. rep. (rapport technique, non publié avant 1976).
- — (1976). **"On bent functions".** In: *Journal of Combinatorial Theory, Series A* 20.3, pp. 300–305.
- Slepian, David (1953). **"On the number of symmetry types of Boolean functions of n variables".** In: *Canadian Journal of Mathematics* 5.2, pp. 185–193.
- Sloane, Neil J. A. and Elwyn R. Berlekamp (1970). **"The weight enumerator for second-order Reed-Muller codes".** In: *IEEE Transactions on Information Theory* IT-16, pp. 745–751.

All refs x

- Sloane, Neil J. A. and R. J. Dick (1971). **"On the enumeration of cosets of first-order Reed-Muller codes".** In: *Proceedings IEEE International Conference on Communications*. Vol. 7. Montreal, pp. 36-2–36-6.
- Sloane, Neil J. A. and Donald S. Whitehead (1970). **"A new family of single-error correcting codes".** In: *IEEE Transactions on Information Theory* IT-16, pp. 717–719.
- Strazdins, Ivars (1997). **"Universal affine classification of Boolean functions".** In: *Acta Applicandae Mathematicae* 46, pp. 147–167.
- Wang, Qichun (2019). **"The covering radius of the Reed-Muller code RM(2,7) is 40".** In: *Discrete Mathematics* 342.12, p. 111625.