



Efficiency of Multidimensional Linear Approximations

04 June 2025



$|0\rangle \rightarrow |1\rangle$

$|0\rangle$

$-H-$

Shishkin Vasily

Outline

1. Task Setting and Hypothesis Formulation
2. Hypothesis Justification
3. Conclusion

[1/3] Task Setting and Hypothesis Formulation

High-Dimensional Linear Approximations

- ▶ F. M. Malyshev, A. V. Erokhin, A. E. Trishin, M. Hermelin, J. Y. Cho, K. Nyberg
- ▶ It is advisable to increase the "informativeness" of statistical analogs. One way to achieve this is by using so-called "multidimensional" statistical analogs
- ▶ Let $F : Q \rightarrow P$, where $Q = \mathbb{F}_{q^n}$ is a degree n extension of the field P , $q = 2^l$, $l \geq 1$.

Bias of Approximation

► $\eta_a F : Q \rightarrow \mathbb{C}^*$, $a \in P$.

$$\eta_a F(x) = \sum_{\alpha \in Q} C_{\alpha}^{\eta_a F} \chi_{\alpha}(x),$$

where $\chi_{\alpha}(x) = \xi^{\text{tr}_S^Q(\alpha x)}$ — character of the group $(Q, +)$

$$C_{\alpha}^{\eta_a F} = \frac{1}{q^n} \sum_{x \in Q} \eta_a F(x) \overline{\chi_{\alpha}(x)}.$$

Bias of Approximation

► $\eta_a F : Q \rightarrow \mathbb{C}^*$, $a \in P$.

$$\eta_a F(x) = \sum_{\alpha \in Q} C_{\alpha}^{\eta_a F} \chi_{\alpha}(x),$$

where $\chi_{\alpha}(x) = \xi^{\text{tr}_S^Q(\alpha x)}$ – character of the group $(Q, +)$

$$C_{\alpha}^{\eta_a F} = \frac{1}{q^n} \sum_{x \in Q} \eta_a F(x) \overline{\chi_{\alpha}(x)}.$$

► Let $N_a(F)$ be a number of solutions in the field Q of equation $F(x) = a \in P$

►
$$\nabla(F, A) = \left(\frac{q}{q-1} \sum_{a \in P} \left(\frac{N_a(F-A)}{q^n} - \frac{1}{q} \right)^2 \right)^{\frac{1}{2}}$$

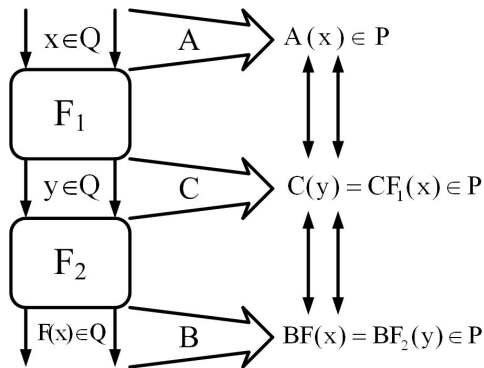
The function $\nabla(F, A)$ satisfies the following properties:

- 1) For any $F, A \in P^Q$: $0 \leq \nabla(F, A) \leq 1$;
- 2) For any $F, A \in P^Q$ the condition $\nabla(F, A) = 1$ is equivalent to:
 $F - A = c \in P$;
- 3) For any $F, A \in P^Q$ the condition $\nabla(F, A) = 0$ is equivalent to: $F - A$ being a uniform function on Q , i.e. $N_a(F - A) = N_b(F - A)$ for any $a, b \in P$;
- 4) For $q = 2$, the following equality holds: $\nabla(F, A) = |\delta_A^F|$, where

$$\delta_A^F = 2 \cdot \mathbf{P}\{F(x) = A(x)\} - 1$$

is the bias of the statistical analog A for the Boolean function F , with probability $\mathbf{P}(\cdot)$ computed under the assumption of a random uniform choice of $x \in Q$.

Bias of a q -valued Statistical Analog for a Composition of Mappings



- **Hypothesis:** The bias $\nabla(BF, A)$ can be estimated by the product $\nabla(CF_1, A) \cdot \nabla(BF_2, C)$.

[2/3] Hypothesis Justification

The Exact Value of the Bias

Theorem

With defined notations it is

$$C_0^{\eta_\beta(BF+A)} = \sum_{C \in L(Q,P)} C_0^{\eta_\beta(CF_1+A)} C_0^{\eta_\beta(BF_2+C)}$$

for any $\beta \in P \setminus \{0\}$, and

$$\nabla^2(BF, A) = \frac{1}{q-1} \sum_{\beta \in P \setminus \{0\}} \left(\sum_{C \in L(Q,P)} C_0^{\eta_\beta(CF_1+A)} C_0^{\eta_\beta(BF_2+C)} \right)^2.$$

The First Bias Estimate

It is natural for $\nabla^2(BF, A)$ to consider the value

$$\tilde{\nabla}_C^2(BF, A) = \frac{1}{q-1} \sum_{\beta \in P \setminus \{0\}} \left(C_0^{\eta_\beta(CF_1+A)} C_0^{\eta_\beta(BF_2+C)} \right)^2,$$

which we call *the first estimate* for bias $\nabla^2(BF, A)$.

Parseval's Equality

The following informal statement is justified, supporting the effectiveness of the first bias estimate: The larger the value of the first bias estimate $\tilde{\nabla}_C^2(BF, A)$, the closer it is to the exact bias value $\nabla^2(BF, A)$.

The Second Bias Estimate

As the bias estimate $\nabla^2(BF, A)$ it is natural to consider the value

$$\tilde{\nabla}_C^2(BF, A) = \nabla^2(BF_2, C) \cdot \nabla^2(CF_1, A),$$

which we call *the second estimate* of bias $\nabla^2(BF, A)$.

Example

1. Let for fixed C one of the functions $BF_2(y) + C(y)$ or $CF_1(x) + A(x)$ be uniform distributed, then

$$\tilde{\tilde{\nabla}}_C^2(BF, A) = \tilde{\nabla}_C^2(BF, A).$$

2. Let for fixed C one of the functions $BF_2(y) + C(y)$ or $CF_1(x) + A(x)$ be constant on P , then

$$\tilde{\tilde{\nabla}}_C^2(BF, A) = \tilde{\nabla}_C^2(BF, A).$$

3. Let for fixed C functions $BF_2(y)$ and $CF_1(x)$ be bent-functions, then

$$\tilde{\tilde{\nabla}}_C^2(BF, A) = \tilde{\nabla}_C^2(BF, A).$$

The Second Bias Estimate

Remark

The closer at least one of the values $\nabla^2(CF_1, A)$ or $\nabla^2(BF_2, C)$ to 1, the smaller the absolute difference between the first and second bias estimates $\nabla^2(BF, A)$ becomes, and thus, the closer the second estimate is to the exact bias value $\nabla(BF, A)$.

Experimental Results

$2t$	$\max \nabla^2(bF^{(2t)}, a)$	$\min \nabla^2(bF^{(2t)}, a)$	$\overline{\nabla^2}(bF^{(2t)}, a)$	$\tilde{\nabla}^2(bF^{(2t)}, a)$
2	0,4804690	0,4804690	0,4804690	0,5017356
4	0,5052080	0,1875000	0,2514260	0,2517387
6	0,5924680	0,0429690	0,1412890	0,1263063
8	0,4087960	0,0085810	0,0843590	0,0633723
10	0,2800910	0,0019800	0,0530650	0,0317962
12	0,2855780	0,0001490	0,0338770	0,0159533
14	0,1657490	0,0000580	0,0229020	0,0080043
16	0,1580730	0,0001510	0,0174250	0,0040161
18	0,0934190	0,0002090	0,0119470	0,0020150
20	0,0584970	0,0000460	0,0092240	0,0010110

[3/3] Conclusion

Conclusion

- ▶ We propose a method for evaluating the "quality" of multidimensional statistical analogs, generalizing the ideas of the one-dimensional linear statistical analogs method
- ▶ It is proven that the natural estimate of the bias of a composition of transformations is close to its true value
- ▶ The results facilitate further research on the multidimensional linear method, both theoretically and practically (constructing multidimensional linear statistical analogs for existing open standardized cipher systems, conducting experimental studies of the method's effectiveness using reduced models)



Any questions?

Shishkin Vasily Alexeevich

Head of Cryptography Laboratory

v.shishkin@kryptonite.ru

