Perfectly Balanced Boolean Functions and Golić Conjecture*

Stanislav V. Smyshlyaev †

Abstract: Golić conjecture ([3]) states that the necessary condition for a function to be perfectly balanced for any choice of a tapping sequence is linearity of a function in the first or in the last essential variable. In the current paper we prove Golić conjecture.

Keywords: Boolean function, perfectly balanced function, keystream generator, filter, Golić conjecture.

1 Introduction

Golić ([3]) studied cryptographic properties of keystream generators consisting of a shift register and a filter function which is connected to the register according to some tapping sequence.

Golić considered model of a keystream generator as a filter with a fixed filter function and arbitrary choice of a tapping sequence. With proposal of an inversion attack on the filter he showed a cryptographic weakness of keystream generators in such model in the case of a filter function being linear either in the first or in the last variable. Earlier Anderson ([1]) proposed an idea of optimum correlation attack and showed corresponding cryptographic weakness of such keystream generators in case of inappropriate choice of both the tapping sequence and the filter function.

The important open question was: do any keystream generators without these undesirable properties exist in Golić model?

Golić conjectured that in his model a filter with a filter function f is invulnerable to Anderson optimum correlation attack if and only if f is linear either in the first or in the last variable. Golić proved an easier part of this conjecture, namely sufficiency, and noted that necessity remained unproven due to a "subtle underlying combinatorial problem remaining to be solved". According to Golić conjecture, the necessary condition for a function to be perfectly balanced (i. e. preserving pure randomness of an input binary sequence when used as a filter function) for any choice of a tapping sequence is linearity of a function in the first or in the last essential variable. Golić conjecture implies that in the model being considered (with

*The work was partially supported by the Russian Foundation for Basic Research (grant no. 09-01-00653)

†Computer Science Department, Lomonosov University, Moscow, Russia; E-mail: smyshsv@gmail.com

independent choice of a tapping sequence and a Boolean function) there are no functions invulnerable both to the inversion attack and to the optimum correlation attack.

To prove Golić conjecture, it suffices to find for arbitrary Boolean function which is nonlinear in the first and in the last essential variables a tapping sequence, such that the Boolean function which describes input-output behaviour of the corresponding filter does not satisfy conditions of the Sumarokov criterion of perfect balancedness ([11]). The trivial case of a function with no linear variables was considered in [7]. In the general case, all linear variables of a function have to be handled in a special way to construct a particular tapping sequence and two binary sequences required by Sumarokov criterion. This in fact solves an underlying combinatorial problem mentioned by Golić.

Related work. Sumarokov ([11]) defined perfect balancedness of Boolean functions. A perfectly balanced filter function transforms uniformly distributed input sequences into uniformly distributed output sequences. Also, Sumarokov proved a useful criterion of perfect balancedness. Dichtl ([2]) offered an example of a Boolean function that is nonlinear in the first and in the last variables but is perfectly balanced when used as a filter function with a certain choice of a tapping sequence. That example does not rule out Golić conjecture because of the fact that some other choices of a tapping sequence do not induce perfect balancedness of corresponding filter functions.

Gouget and Sibert ([4]) suggested not to consider a Boolean function independently of a tapping sequence used in a filter and noted that one class of perfectly balanced functions nonlinear in both the first and the last variable was described by Logachev ([6]). Nevertheless, existence of this class is not in conflict with Golić conjecture either, because the models are different.

2 Definitions

As usual, $\mathbb{F}_2$ denotes the Galois field. For any $n \in \mathbb{N}$ V_n denotes $\mathbb{F}_2^n$, $\mathcal{F}_n$ is the set of all Boolean functions in n variables. Variable x_i is called essential for the function $f(x_1, x_2, \ldots, x_n) \in \mathcal{F}_n$ if there exists $(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n) \in \mathrm{V}_{n-1}$ such that $f(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \neq f(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$. Variable x_i is called linear essential for the function $f(x_1, x_2, \ldots, x_n) \in \mathcal{F}_n$ if for any $(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n) \in \mathrm{V}_{n-1}$ inequality $f(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \neq f(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$ holds. By Φ_n, $\Phi_n \subset \mathcal{F}_n$, we denote the set of all Boolean functions with both first and last variables being essential.

Let $m \in \mathbb{N}$. Boolean function $g \in \mathcal{F}_N$, $N \in \mathbb{N}$, induces mapping $g_m \colon \mathrm{V}_{m+N-1} \to \mathrm{V}_m$ of the form

$$g_m(z_1, z_2, \ldots, z_{m+N-1}) = (g(z_1, \ldots, z_N), g(z_2, \ldots, z_{N+1}), \ldots, g(z_m, \ldots, z_{m+N-1})). \qquad (2.1)$$

Let $\gamma = (\gamma_1, \ldots, \gamma_n)$ be a tuple of nonnegative integers such that $\gamma_1 = 0; \gamma_{i+1} > \gamma_i, i = 1, 2, \ldots, n-1$, and let $N = \gamma_n + 1$. From now on we consider tuples γ of this form. For γ of the above form and arbitrary $f \in \Phi_n$ we denote $f(x_{N-\gamma_n}, x_{N-\gamma_{n-1}}, \ldots, x_{N-\gamma_1})$ by $f_\gamma(x_1, \ldots, x_N)$.

A filter with a tapping sequence γ, and a filter function f is a mapping of the set $\bigcup\limits_{i=\gamma_n+1}^{\infty} \mathrm{V}_i$ to $\bigcup\limits_{i=1}^{\infty} \mathrm{V}_i$, defined by equations (2.1) with $m = 1, 2, \ldots$ and $g = f_\gamma$.

Definition 2.1. ([11]). A Boolean function $f \in \mathcal{F}_n$ is said to be perfectly balanced if for any $m \in \mathbb{N}$ and any $y \in \mathrm{V}_m$

$$\sharp(f_m)^{-1}(y) = 2^{n-1},$$

where $\sharp$ denotes cardinality.

The subset of $\mathcal{F}_n$ composed by all functions linear in the first (resp. last) variable is denoted by $\mathcal{L}_n$ (resp. $\mathcal{R}_n$). It is easy to see ([11]) that all functions in $\mathcal{L}_n \cup \mathcal{R}_n$ are perfectly balanced.

3 Preliminaries

We denote the set of all perfectly balanced n-variable functions by $\mathcal{PB}_n$, $\mathcal{PB}_n \subseteq \mathcal{F}_n$. From cryptographic applications point of view the subset $\Phi_n \cap \mathcal{PB}_n \setminus (\mathcal{L}_n \cup \mathcal{R}_n)$ is of primary importance.

The next theorem states necessary and sufficient condition for an m-tuple in the right-hand side of equation (2.1) to be distributed uniformly in V_m given the uniform distribution of the vector $X_m = (x_1, \ldots, x_{m+n-1})$ and can be easily proven using only Definition 2.1 and basics of probability theory.

Theorem 3.1. *Let $n \in \mathbb{N}$ and $f \in \mathcal{F}_n$. Let $\{X_m = (x_1, \ldots, x_{m+n-1})\}_{m=1}^{\infty}$ be a sequence of random vectors with distribution*

$$\Pr\{X_m = (a_1, \ldots, a_{m+n-1})\} = 2^{-(m+n-1)}$$

for any $(a_1, \ldots, a_{m+n-1}) \in \mathrm{V}_{m+n-1}$. Random vector $Y_m = f_m(X_m)$ is distributed uniformly for each $m \in \mathbb{N}$ iff f is perfectly balanced.

Theorem 3.2. *([11]). A Boolean function $f \in \mathcal{F}_n$ is perfectly balanced iff there is no pair of distinct binary sequences*

$$x = (x_1, \ldots, x_r), z = (z_1, \ldots, z_r) \in \mathrm{V}_r, r > 2n, \tag{3.1}$$

such that

$$x_1 = z_1, \ldots, x_n = z_n, x_{r-n+1} = z_{r-n+1}, \ldots, x_r = z_r; \tag{3.2}$$

$$x \neq z; \tag{3.3}$$

$$f(x_i, \ldots, x_{i+n-1}) = f(z_i, \ldots, z_{i+n-1}), i = 1, \ldots, r-n+1. \tag{3.4}$$

Full proof of the Theorem 3.2 can be found in Appendix A.

Theorem 3.3. *([3]) For a filter with a filter function f for any choice of a tapping sequence γ the output sequence is purely random given that the input sequence is such if (and only if [not proven]) $f(z_1, \ldots, z_n)$ is balanced for each value of $(z_2, \ldots, z_n)$ (i. e. f is linear in the first variable) or $f(z_1, \ldots, z_n)$ is balanced for each value of $(z_1, \ldots, z_{n-1})$ (i. e. f is linear in the last variable).*

According to Dichtl ([2]), unproven necessary condition in Theorem 3.3 is referred to as Golić conjecture.

4 Main Result

Theorem 3.1 implies that Golić conjecture can be stated in the following form.

Conjecture 4.1. If f_γ is perfectly balanced for every possible choice of γ, then f is linear in the first or in the last variable.

To prove Golić conjecture it suffices to construct for arbitrary $f \in \Phi_n \setminus (\mathcal{L}_n \cup \mathcal{R}_n)$ a particular tapping sequence making function f_γ not perfectly balanced. The key idea is to force γ_i increase exponentially in i. After choosing appropriate γ we construct two different binary sequences of the special form required by Sumarokov criterion (Theorem 3.2) to prove that f_γ is not perfectly balanced.

Theorem 4.2.
For any $f \in \Phi_n \setminus (\mathcal{L}_n \cup \mathcal{R}_n)$ *there exists a tuple* γ *such that* $f_\gamma \notin \mathcal{PB}_N$.

Proof.
Let $f \in \Phi_n \setminus (\mathcal{L}_n \cup \mathcal{R}_n)$. Suppose that f depends on each variable essentially (this is w.l.o.g. since we are free to choose any tuple γ).
Choose γ as follows: $\gamma = (\tau_0, \tau_0 + \delta_0, \ldots, \tau_0 + (m_0 - 1)\delta_0, \tau_1, \ldots, \tau_k, \tau_k + \delta_k, \ldots, \tau_k + (m_k - 1)\delta_k,\ \tau_{k+1}, \ldots, \tau_{n-l-1})$, where $\delta_k = \frac{\tau_{k+1} - \tau_k}{m_k}$ and $m_k - 1$ is the number of succeeding linear essential variables of f between $(n-l-k-1)$th and $(n-l-k)$th nonlinear essential variables, $k = 0, 1, \ldots, n-l-2$; $l = (m_0 - 1) + \ldots + (m_{n-l-1} - 1)$ is the total number of linear essential variables of f. Let $m = \max\limits_{k=0,\ldots,n-l-2} m_k$, $\tau_0 = 0, \tau_1 = m_0, \tau_{k+1} > (4m^2 + 1)\tau_k, k = 1, \ldots, n-l-2$ and $\tau_{k+1} - \tau_k$ be a multiple of m_k.
Consider two binary sequences $y = (y_0, \ldots, y_M), z = (z_0, \ldots, z_M), M = 2N + \sum\limits_{j=1}^{l'} \delta_{k_j}$, where k_j are indices such that $m_{k_j} > 1$ (l' denotes the total number of these indices). Fix certain bits of these sequences as follows: $y_{N + \sum\limits_{j=1}^{l'} a_j \delta_{k_j}} = 0, z_{N + \sum\limits_{j=1}^{l'} a_j \delta_{k_j}} = 1$, $\forall a_j \in \{0, 1\}, j = 1, \ldots, l'$.
Indices of the form $N + \sum\limits_{j=1}^{l'} a_j \delta_{k_j}$ are referred to as B-indices and all the others as A-indices. It is easy to conclude using Theorem 3.2, that to prove the Theorem it suffices to show that one can set all yet unfixed bits of y so that $f_{\gamma M-N+2}(y) = f_{\gamma M-N+2}(z)$ and $z_j = y_j$ holds for any A-index j. Thereby we have distinct binary sequences y, z, $|y| = |z| > 2N$, with coinciding leading as well as tailing N-bit subsequences and such that $f_{\gamma M-N+2}(y) = f_{\gamma M-N+2}(z)$. Then, using Theorem 3.2, one concludes that γ is required tapping sequence, $f_\gamma \notin \mathcal{PB}_N$ and the Theorem follows.
First, we demonstrate some simple relations.

1. $\delta_k = \frac{\tau_{k+1} - \tau_k}{m_k} > \frac{(1+4m^2)\tau_k - \tau_k}{m_k} \geqslant 4m\tau_k.$
2. If $m_{k-1} > 1$, then $\tau_k = \tau_{k-1} + m_{k-1}\delta_{k-1} \geqslant 2\delta_{k-1}.$
3. $\delta_k > \delta_{k-1}$. From 1 and 2 it follows that if $m_{k-1} > 1$, then $\delta_k > 8m\delta_{k-1}.$

4. From 3 it follows that $\sum\limits_{j=j'}^{l'} \delta_{k_j} < \sum\limits_{j=j'}^{l'} \delta_{k_{l'}} \frac{1}{(8m)^{l'-j}} < \sum\limits_{i=0}^{\infty} \delta_{k_{l'}} \frac{1}{(8m)^i} = \frac{\delta_{k_{l'}}}{1-\frac{1}{8m}} = \delta_{k_{l'}} \frac{8m}{8m-1}$.

5. $\delta_k = \frac{\tau_{k+1}-\tau_k}{m_k} < \frac{\tau_{k+1}}{m_k} \leqslant \tau_{k+1}$ if $k \geqslant 1$; $\delta_0 \leqslant \tau_1$.

According to Theorem 3.2, to prove the Theorem it suffices to prove solvability of the following system of equations.

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} f_\gamma(y_0, \ldots, y_{N-1}) = f_\gamma(z_0, \ldots, z_{N-1}) \\ \ldots \\ f_\gamma(y_{M-N+1}, \ldots, y_M) = f_\gamma(z_{M-N+1}, \ldots, z_M) \end{array} \right. \\ \left\{ \begin{array}{l} y_{N+\sum\limits_{j=1}^{l'} a_j \delta_{k_j}} = 0, \forall a_j \in \{0,1\}, j = 1, \ldots, l' \\ z_{N+\sum\limits_{j=1}^{l'} a_j \delta_{k_j}} = 1, \forall a_j \in \{0,1\}, j = 1, \ldots, l' \\ y_t = z_t, t \neq N + \sum\limits_{j=1}^{l'} a_j \delta_{k_j}, \forall a_j \in \{0,1\}, j = 1, \ldots, l' \end{array} \right. \end{array} \right. \tag{4.1}$$

Now we fix variables involved in the second subsystem of (4.1) and consider ith equation ($i = 0, \ldots, M - N + 1$) of the first subsystem. Three cases are possible.

Case 1. Each B-index variable, which is essential for $f_\gamma^i \equiv f_\gamma(y_i, \ldots, y_{i+N-1})$, is linear for f_γ^i.

In Lemma 4.3 (the proof can be found in Appendix B) we prove that in this case f_γ^i depends on exactly two such variables. Then, from definition of linear dependence and from our fixation of B-index variables, we get that ith equation of the first subsystem turns out to be identity.

Lemma 4.3. Let the set of B-index variables that are essential for f_γ^i be nonempty, and let f_γ^i be linear in any B-index variable. Then f_γ^i is linear in exactly two B-index variables.

Case 2. f_γ^i depends essentially on no B-index variable.

In this case we have a trivial equality, since variables with equal A-indices are equal, i.e. $y_j = z_j, j \neq N + \sum\limits_{j=1}^{l'} a_j \delta_{k_j}$.

Case 3. f_γ^i depends essentially and nonlinearly on some B-index variable $y_{\bar{j}^i}$.

Lemma 4.4 (the proof is in Appendix C) states that in this case f_γ^i is nonlinear in exactly one essential B-index variable. In other words, if any other B-index variable is essential for f_γ^i, then the latter is linear essential variable of f_γ^i.

Lemma 4.4. If f_γ^i depends essentially and nonlinearly on some B-index variable, then there is exactly one such (nonlinear, essential, B-index) variable.

Therefore ith equation of the system could be written in the form

$$\phi(y_{j_1^i}, y_{j_2^i}, \ldots, y_{\bar{j}^i-1}, 0, y_{\bar{j}^i+1}, \ldots, y_{j_{n-l}^i}) = \phi(y_{j_1^i}, y_{j_2^i}, \ldots, y_{\bar{j}^i-1}, 1, y_{\bar{j}^i+1}, \ldots, y_{j_{n-l}^i}) \oplus \zeta_i,$$

where ϕ is the function constructed from f by setting all linear essential variables to zero; $(y_{j_1^i}, y_{j_2^i}, \ldots, y_{\bar{j}^i-1}, y_{\bar{j}^i+1}, \ldots, y_{j_{n-l}^i})$ are yet unfixed variables and ζ_i is a constant. The variable $y_{\bar{j}^i}$ is essential and nonlinear for ϕ, thus there exists at least one setting of variables $(y_{j_1^i}, y_{j_2^i}, \ldots, y_{\bar{j}^i-1}, y_{\bar{j}^i+1}, \ldots, y_{j_{n-l}^i})$, which turns i th equation of the first subsystem of system (4.1) to identity. The Theorem is proven if one shows that no indices j_m^i appear in any other equation whose function satisfies conditions of the Case 3. In other words, each index of a nonlinear essential variable of f_γ^i appears in at most one equation with function f_γ^i depending essentially and nonlinearly on a B-index variable. This fact is proven in Lemma 4.5 (the proof is in Appendix D).

Lemma 4.5. There is no index of a nonlinear essential variable of f_γ^j (for any j) that occurs in at least two equations with functions f_γ^i satisfying conditions of the Case 3.

Also, each variable, that is present in equations corresponding to Case 3, is present only in one such equation. Equations which correspond to Case 1 and Case 2 turn into trivial equalities, and each equation corresponding to Case 3 is solvable. So, we can conclude that the whole system is solvable, and that fact directly implies statement of the Theorem. □

Remark 4.6. Proof of Theorem 4.2 is much easier in the case of f without linear essential variables. In this case one has $m_k = 1$, $k = 0, \ldots, n-1$; the sequences y, z are of length $2N+1$ and differ in one bit only.

5 Conclusion and Open Question

Theorem 4.2 implies the negative answer to the question of existence (in Golić model) of keystream generators without undesirable properties mentioned in introduction. But our proof is based on a register whose size exponentially grows with the number of taps. Thus, though theoretically the question with Golić conjecture is now closed, there remains the following open question: whether it is possible to prove a similar statement without forcing sequence γ increase exponentially (e. g. in the model where the size of a register is bounded by some polynomial).

References

[1] R.J.Anderson. Searching for the Optimum Correlation Attack. B. Preneel (ed.) Fast Software Encryption. LNCS, vol. 1008, pp. 137-143. Springer, Heidelberg (1995).

[2] M. Dichtl. On nonlinear filter generators. E. Biham (ed.) FSE 1997. LNCS, vol. 1267, pp. 103-106. Springer, Heidelberg (1997).

[3] Dj.Golić, J. On the Security of Nonlinear Filter Generators. D. Gollmann (ed.) Proceedings of Fast Software Encryption 1996. LNCS, vol. 1039, pp. 173-188. Springer, Heidelberg (1996).

[4] A.Gouget, H.Sibert. Revisiting Correlation-Immunity in Filter Generators. C.Adams, A.Miri and M.Wiener(Eds.) Proceedings of SAC 2007, LNCS, vol. 4876, pp. 378-395. Springer, Heidelberg (2007).

[5] D. A. Huffman. Canonical Forms for Information-Lossless Finite-State Logical Machines. IRE Trans. Circuit Theory, 1959, v. 5, spec. suppl., p. 41-59.

[6] O.A. Logachev, On perfectly balanced Boolean functions. Cryptology ePrint Archive, Report 2007/022, http://eprint.iacr.org/.

[7] O.A. Logachev, A.A. Salnikov, S.V. Smyshlyaev, V.V. Yashchenko. Perfectly Balanced Functions in Symbolic Dynamics. Cryptology ePrint Archive, Report 2009/296, http://eprint.iacr.org/.

[8] O.A. Logachev, A.A. Salnikov, and V.V. Yashchenko, Boolean Functions in Coding Theory and Cryptology, MCCME, Moscow, 2004 (in Russian).

[9] O.A. Logachev, S.V. Smyshlyaev, V.V. Yashchenko. New methods of investigation of perfectly balanced Boolean functions. Discrete Mathematics and Applications. Volume 19, Issue 3, Pages 237–262, ISSN (Online) 1569-3929, ISSN (Print) 0924-9265, DOI: 10.1515/DMA.2009.014, /July/2009.

[10] F.P. Preparata. Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties. IEEE Trans. Electron. Comput., 1966, v.15, N6, pp. 898-909.

[11] S.N. Sumarokov, Functions of defect zero and invertability of some class of finite-memory encoders, Obozrenie prom. i prikl. mat. 1(1) (1994) 33-55 (in Russian).

Appendix A

Proof of Theorem 3.2. Denote by $\gamma(f,l)$ the maximum possible (over all $(y_1,y_2,\ldots,y_l)\in \mathrm{V}_l$) number of solutions to the system

$$\begin{cases} f(x_s,x_{s+1},\ldots,x_{s+n-1}) = y_s \\ s=1,2,\ldots,l. \end{cases} \tag{5.1}$$

It is obvious that if for some f there are no sequences x, z such that (3.1)-(3.4) hold, then the output sequence $(y_1,y_2,\ldots,y_{r-n+1}) = f_{r-n+1}(x)$ and $x_1,x_2,\ldots,\ x_n;x_{r-n+1},\ldots,x_r$ determine the whole input sequence x, and so, for any integer l, $\gamma(f,l)\leqslant 2^{2n-2}$. It is easy to show that in the opposite case $\gamma(f,l)$ is unbounded as a function of l with $l\to\infty$.

In the remaining part of the proof it is shown that $\gamma(f,l)$ is bounded (with $l\to\infty$) iff f is perfectly balanced.

By definition, for any $f\in\mathcal{PB}_n$ and any natural l $\gamma(f,l)=2^{n-1}$, i.e. $\gamma(f,l)$ is not unbounded with $l\to\infty$. Let $f\notin\mathcal{PB}_n$. Then there is an integer l and a tuple $\widetilde{y}=(\widetilde{y}_1,\widetilde{y}_2,\ldots,\widetilde{y}_l)^\top\in\mathrm{V}_l$, such that there exist $2^{n-1}+\alpha$ solutions to (5.1), where $\alpha\geqslant 1$.

For the tuple $\widetilde{y}\in\mathrm{V}_l$ construct the set of all possible sequences of length $(k+1)l+k(n-1)$ of the following form:

$$\widetilde{y}_1,\ldots,\widetilde{y}_l,y_{l+1},\ldots,y_{l+n-1},\widetilde{y}_1,\ldots,\widetilde{y}_l,y_{2l+n-1},\ldots,y_{2l+2(n-1)},\ldots \\ \ldots,y_{kl+(k-1)(n-1)+1},\ldots,y_{kl+k(n-1)},\widetilde{y}_1,\ldots,\widetilde{y}_l, \tag{5.2}$$

$k=1,2,\dots$, where $y_i \in \mathbb{F}_2, i=l+1,l+2,\dots,l+n-1; 2l+n-1, 2l+n-2,\dots$. Let μ_k denote the average number of inputs of $f_{(k+1)l+k(n-1)}$ that correspond to one output of the form (5.2). In this case,

$$\mu_k = 2^{n-1}(1+\frac{\alpha}{2^{n-1}})^{k+1},$$

so $\mu_k \to \infty$ with $k \to \infty$. That is, for any integer M there is an integer $k=k(M)$ such that $\mu_{k(M)} > M$, i.e. preimage of one of the sequences (5.2) of length $t(M)=(k(M)+1)l+k(M)(n-1)$ is of cardinality greater than M. This means that for arbitrary M there exists $t(M)$ such that $\gamma(f,t(M)) > M$ and thus $\gamma(f,l)$ is unbounded as a function of l. $\square$

Appendix B

Proof of Lemma 4.3. Consider the set of all essential B-index variables of f_γ^i and let the variable in this set with the maximal B-index correspond to the $(N-\tau_k-r\delta_k)$ th variable of f_γ, $1 \leqslant r \leqslant m_k-1$. It is evident that in this case there is another B-index variable corresponding to $(N-\tau_k-(r+1)\delta_k)$ th variable of f_γ. According to conditions of Case 1, this variable is linear as well. Therefore $1 \leqslant r \leqslant m_k-2, m_k \geqslant 3$. Next one has to prove that no other B-index variable is essential for f_γ^i.

It suffices to show that variables of f_γ with indices $N-\tau_k-r\delta_k-\sum\limits_{j=1}^{l'} b_j\delta_{k_j}$, $b_j \in \{-1,0,1\}$, $j=1,\dots,l'$ are not essential for f_γ except for two trivial cases ($\sum\limits_{j=1}^{l'} b_j\delta_{k_j} = \delta_k$ and $\sum\limits_{j=1}^{l'} b_j\delta_{k_j} = 0$).

Let $k_{j^*}=k$. Two cases are possible.

1) $\exists j^\circ > j^* : b_{j^\circ} \neq 0$ and let j° be the maximal index j such that $b_j \neq 0$. Evidently, it suffices to consider the case of $b_{j^\circ}=1$. Then $N-\tau_k-r\delta_k-\sum\limits_{j=1}^{l'} b_j\delta_{k_j} \leqslant N-\tau_k-r\delta_k-\delta_{k_{j^\circ}}+\sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} < N-\tau_k-r\delta_k-4m(1-\frac{1}{8m-1})\tau_{k_{j^\circ}} < N-\tau_{k_{j^\circ}}$.

Also, the following inequality holds. $N-\tau_k-r\delta_k-\sum\limits_{j=1}^{l'} b_j\delta_{k_j} = N-(\tau_{k+1}-(m_k-r)\delta_k)-\sum\limits_{j=1}^{l'} b_j\delta_{k_j} \geqslant N-(\tau_{k+1}-2\delta_k)-\sum\limits_{j=1}^{l'} b_j\delta_{k_j} \geqslant N-(\tau_{k+1}-2\delta_k)-\sum\limits_{j=1}^{j^\circ}\delta_{k_j} > N-(\tau_{k+1}-2\delta_k)-\delta_{k_{j^\circ-1}}\frac{8m}{8m-1}-\delta_{k_{j^\circ}}$. If $k_{j^\circ}-1=k$, then $k_{j^\circ-1}=k$ and one can estimate the last expression as follows: $N-(\tau_{k+1}-2\delta_k)-\delta_{k_{j^\circ-1}}\frac{8m}{8m-1}-\delta_{k_{j^\circ}} = N-\tau_{k+1}+\delta_k-\frac{\delta_k}{8m-1}-\delta_{k+1} > N-\tau_{k+1}-\delta_{k+1} = N-\tau_{k_{j^\circ}}-\delta_{k_{j^\circ}}$. Else $N-(\tau_{k+1}-2\delta_k)-\delta_{k_{j^\circ-1}}\frac{8m}{8m-1}-\delta_{k_{j^\circ}} > N-\tau_{k+1}-\delta_{k_{j^\circ-1}}\frac{8m}{8m-1}-\delta_{k_{j^\circ}} \geqslant N-\tau_{k+1}-\delta_{k_{j^\circ}-1}\frac{8m}{8m-1}-\delta_{k_{j^\circ}} \geqslant N-\tau_{k_{j^\circ}-1}-\delta_{k_{j^\circ}-1}\frac{8m}{8m-1}-\delta_{k_{j^\circ}} > N-\delta_{k_{j^\circ}-1}(\frac{1}{4m}+\frac{8m}{8m-1})-\delta_{k_{j^\circ}} = N-\frac{\tau_{k_{j^\circ}}-\tau_{k_{j^\circ}-1}}{m_{k_{j^\circ}}}(\frac{1}{4m}+\frac{8m}{8m-1})-\delta_{k_{j^\circ}} > N-\frac{\tau_{k_{j^\circ}}}{m_{k_{j^\circ}}}(\frac{1}{4m}+1+\frac{1}{8m-1})-\delta_{k_{j^\circ}} \geqslant N-\frac{\tau_{k_{j^\circ}}}{m_{k_{j^\circ}}}(\frac{1}{12}+1+\frac{1}{23})-\delta_{k_{j^\circ}} \geqslant N-\frac{\tau_{k_{j^\circ}}}{2}(\frac{1}{12}+1+\frac{1}{23})-\delta_{k_{j^\circ}} > N-\tau_{k_{j^\circ}}-\delta_{k_{j^\circ}}$. This implies that all the variables with indices $j^\circ > j^*, b_{j^\circ}=1$ occur in the interval $(N-\tau_{k_{j^\circ}}-\delta_{k_{j^\circ}}, N-\tau_{k_{j^\circ}})$ and thus could not be essential for f_γ.

2) $\forall j > j^* \Rightarrow b_j = 0$; $\exists j^\circ < j^* : b_{j^\circ} \neq 0$ (if there are multiple such j°, we choose the largest one).

If $b_{j^*} = 1$, then $N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} > N - \tau_k - r\delta_k - \frac{8m}{8m-1}\delta_k > N - \tau_k - (r+2)\delta_k$; $N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} < N - \tau_k - r\delta_k, N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} \neq N - \tau_k - (r+1)\delta_k.$

If $b_{j^*} = 0$, then $N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} > N - \tau_k - r\delta_k - \frac{1}{8m-1}\delta_k > N - \tau_k - (r+1)\delta_k$; $N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} < N - \tau_k - (r-1)\delta_k, N - \tau_k - r\delta_k - \sum_{j=1}^{l'} b_j\delta_{k_j} \neq N - \tau_k - r\delta_k.$

Thus, in this case variables are not essential too. □

Appendix C

Proof of Lemma 4.4. By contradiction, let for some f_γ^i two B-index variables correspond to $(N-\tau_k)$ th and $(N-\tau_p)$ th variables of f_γ, $p > k$. Then

$$\tau_p - \tau_k = \sum_{j=1}^{l'} b_j\delta_{k_j}, b_j \in \{-1, 0, 1\}. \tag{5.3}$$

1) Let the set $K = \{j | k_j \geqslant p, b_j = 1\}$ be nonempty and let j° be the maximum element of this set. Then $\sum_{j=1}^{l'} b_j\delta_{k_j} \geqslant \delta_{k_{j^\circ}} - \sum_{j=1}^{j^\circ-1} \delta_{k_j} > \delta_{k_{j^\circ}} - \frac{8m}{8m-1}\delta_{k_{j^\circ-1}} > \delta_{k_{j^\circ}}(1 - \frac{1}{8m-1}) > 4m(1 - \frac{1}{8m-1})\tau_p > \tau_p - \tau_k$.

2) Let K be empty, i.e. $b_{j^\circ} \leqslant 0, k_{j^\circ} \geqslant p$. Then $\sum_{j=1}^{l'} b_j\delta_{k_j} \leqslant \sum_{j=1}^{j_p} \delta_{k_j} < \frac{8m}{8m-1}\delta_{k_{j_p}}$, where $k_{j_p} \leqslant p-1$. $\frac{8m}{8m-1}\delta_{k_{j_p}} = \frac{8m}{8m-1}\frac{\tau_{k_{j_p}+1} - \tau_{k_{j_p}}}{m_{k_{j_p}}} \leqslant \frac{8}{7}\frac{\tau_{k_{j_p}+1} - \tau_{k_{j_p}}}{2} \leqslant \frac{8}{7}\frac{\tau_p - \tau_{p-1}}{2} < \tau_p - \tau_{p-1} \leqslant \tau_p - \tau_k$.

Hence, (5.3) is impossible and this concludes the proof of the Lemma. □

Appendix D

Proof of Lemma 4.5. We have to prove that equality

$$\tau_a - \tau_b + \sum_{j=1}^{l'} a'_j\delta_{k_j} = \tau_c - \tau_d + \sum_{j=1}^{l'} a''_j\delta_{k_j} \tag{5.4}$$

does not hold if conditions

$$\begin{cases} \tau_a = \tau_c \\ \tau_b = \tau_d \\ a'_j = a''_j, j = 1, \dots, l' \end{cases} \tag{5.5}$$

are not satisfied.

First, we prove that equality $\sum\limits_{j=1}^{l'} a'_j\delta_{k_j} = \sum\limits_{j=1}^{l'} a''_j\delta_{k_j}$ holds only if $a'_j = a''_j, j = 1,\dots,l'$. Let $a'_{j^\circ} \neq a''_{j^\circ}$, $a'_{j^\circ} = 1, a''_{j^\circ} = 0$ and let j° be the largest index such that $a'_j \neq a''_j$. Then

$$\sum_{j=1}^{l'} a'_j\delta_{k_j} - \sum_{j=1}^{l'} a''_j\delta_{k_j} = \delta_{k_{j^\circ}} + \sum_{j=1}^{j^\circ-1} a'_j\delta_{k_j} - \sum_{j=1}^{j^\circ-1} a''_j\delta_{k_j} \geqslant$$
$$\geqslant \delta_{k_{j^\circ}} - \sum_{j=1}^{j^\circ-1} a''_j\delta_{k_j} \geqslant \delta_{k_{j^\circ}} - \sum_{j=1}^{j^\circ-1} \delta_{k_j} > \delta_{k_{j^\circ}} - \tfrac{1}{8m-1}\delta_{k_{j^\circ}} > 0.$$

Consider indices $a, b, c, d, e+1$, $e = k_{j^\circ}$, where j° is the largest index such that $a'_j \neq a''_j$. One can transform (5.4) as follows: $\tau_a - \tau_b = \tau_c - \tau_d + \sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j}, b_j = a''_j - a'_j, j = 1,\dots,j^\circ$.

Let $q = \max\{a, b, c, d, e+1\}$. We have (up to equivalence) five possibilities.

1) $q = a, q > b, q > c, q > d, q > e+1$. Then $\tau_a = \tau_q > (4m^2+1)\tau_{q-1} \geqslant 5\tau_{q-1} \geqslant \tau_b + (\tau_c - \tau_d) + 3\tau_{q-1} \geqslant \tau_b + \tau_c - \tau_d + 3\delta_{q-2} > \tau_b + \tau_c - \tau_d + \delta_{q-2}\frac{8m}{8m-1} > \tau_b + \tau_c - \tau_d + \sum\limits_{j=1}^{j^\circ}\delta_{k_j} \geqslant \tau_b + \tau_c - \tau_d + \sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j}$, hence equality (5.4) does not hold.

2) $q = e+1, a \leqslant e, b \leqslant e, c \leqslant e, d \leqslant e$. Let $b_{j^\circ} = 1$ (the case of $b_{j^\circ} = -1$ is treated along the same lines). $\delta_e > 4m\tau_e > 2\tau_e + 2\delta_{e-1} > (\tau_a - \tau_b + \tau_d - \tau_c) + \delta_{e-1} + \frac{1}{8m-1}\delta_{e-1} > \tau_a - \tau_b + \tau_d - \tau_c + \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} \geqslant \tau_a - \tau_b + \tau_d - \tau_c + \sum\limits_{j=1}^{j^\circ-1} b_j\delta_{k_j}$, thus equality (5.4) does not hold.

3) $q = a = c$. Then (5.4) can be transformed into $\tau_d = \tau_b + \sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j}$. If $b = d$, then (5.4) turns into $\sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j} = 0$, which holds only if $b_j = 0, j = 1,\dots,j^\circ$.

If $d > b$ (or $d < b$, that can be treated similarly), we denote $q' = \max\{b, d, e+1\}$ and consider three subcases.

- $d = q' > e+1$. Then $\tau_d > (4m^2+1)\tau_{q'-1} > \tau_b + 4m^2\tau_{q'-1} > \tau_b + 4m^2\delta_e > \tau_b + \frac{8m}{8m-1}\delta_e > \tau_b + \sum\limits_{j=1}^{j^\circ}\delta_{k_j} \geqslant \tau_b + \sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j}$.

- $q' = e+1 > d$. Then $\sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j} > 4m\tau_{q'-1} - \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} \geqslant \tau_d + \tau_b + 2\tau_{q'-1} - \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} > \tau_d + \tau_b + 2\delta_{q'-2} - \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} = \tau_d + \tau_b + 2\delta_{e-1} - \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} > \tau_d + \tau_b + \frac{8m}{8m-1}\delta_{k_{j^\circ-1}} - \sum\limits_{j=1}^{j^\circ-1}\delta_{k_j} > \tau_d + \tau_b$.

- $q' = e+1 = d$. Then $\tau_d > \frac{3}{4}\tau_d + m^2\tau_{q'-1} \geqslant \frac{3\tau_{e+1}}{2m_{j^\circ}} + \tau_b > \frac{8m}{8m-1}\delta_e + \tau_b > \tau_b + \sum\limits_{j=1}^{j^\circ}\delta_{k_j} \geqslant \tau_b + \sum\limits_{j=1}^{j^\circ} b_{k_j}\delta_{k_j}$.

In fact, other subcases are possible but each of them is equivalent to one of the above.

4) $q = a = d, b < q, c < q$. Then $e+1 \leqslant q$ and hence $\tau_a + \tau_d > (4m^2+1)\tau_{q-1} + \tau_q > \tau_c + \tau_b + \tau_q \geqslant \tau_c + \tau_b + 2\delta_e > \tau_c + \tau_b + \frac{8m}{8m-1}\delta_e > \tau_c + \tau_b + \sum\limits_{j=1}^{j^\circ} b_j \delta_{k_j}$, thus (5.4) does not hold in this case either.

5) $q = a = e+1, b < q, c < q, d < q$. Then $\tau_a = \frac{3\tau_a}{4} + \frac{\tau_a}{4} > \frac{3\tau_{e+1}}{4} + m^2\tau_{q-1}$. $e = k_{j^\circ}$, so $m_e \geqslant 2, m \geqslant 2$. Then $\frac{3\tau_{e+1}}{4} + m^2\tau_{q-1} > \frac{3\tau_{e+1}}{2m_e} + 3\tau_{q-1} > \frac{3}{2}\delta_e + 3\tau_{q-1} > (1 + \frac{1}{8m-1})\delta_e + \tau_b + (\tau_c - \tau_d) > \sum\limits_{j=1}^{j^\circ} \delta_{k_j} + \tau_b + (\tau_c - \tau_d) \geqslant \sum\limits_{j=1}^{j^\circ} b_j\delta_{k_j} + \tau_b + \tau_c - \tau_d$. This implies that (5.4) does not hold in this case either. $\square$