Errata and clarifications

p. 4 By *by* $\mathbb{F}_{p^n}$ *we shall mean the unique finite field with* p^n *elements*, we mean that we shall fix one concrete representation of a finite field.

p. 5 In Definition 3 there should $\mathbb{F}_2$ is *codomain* of f, instead of image.

pp. 5–6 The fact, that univariate algebraic normal form corresponds to multivariate normal form can be seen from a simple counting argument.

p. 6 In Definition 8 the $wt(j)$ denotes the Hamming weight of j. In this case it means the number of nonzero digits in j, when j is written in binary form. Also the notion of multivariate degree (as opposed to univariate degree) is independent on the chosen basis of $\mathbb{F}$.

p. 7 It makes sense to define kernel of a linearized polynomial, or an adjoint polynomial, since linearized polynomials correspond to linear mappings.

p. 8 In the proof of Lemma 1 we are not using *freshman's dream*, but simply the fact, that in $\mathbb{F}_{2^n}$ it hold for every c that $c^{2^n} = c$.

p. 9 In Definition 12 (Walsh transform) it should be noted, that the codomain of Walsh transform are integers, and therefore the sum in the definition is evaluated over $\mathbb{Z}$.

At the end of the penultimate paragraph the linear functions are meant to be only the functions f such that $f(0) = 0$. Affine functions are then functions of multivariate degree 1 such that $f(0) \neq 0$.

The maximal values of $\hat{f}(u, v)$ for $f = ax$ linear can be seen from the fact, that there exists one linear function that has the same value as f – indeed it is $f = ax$ itself. The value of $\hat{f}(a, 1)$ will then be 2^n.

p. 10 In Lemma 6 the notation $max(|W_f|)$ means: $max(|a| : a \in W_f)$.

p. 11 In Definition 15 there should be: *We say, that* f *is plateaued if there exists a single* $k \in \mathbb{N}$ *such that in the Walsh spectrum of* f *the only values are 0 and* $\pm 2^k$.

In Lemma 7 λ is indeed an integer.

p. 12 In Definition 19 there should be a sign of equality instead of inequality: $\mathrm{B}_f = \{v \in \mathbb{F} : \hat{f}(0, v) = \pm 2^{n/2}\}$

In Definition 20 there should be a sign of inequality instead of equality: $\mathrm{NB}_f = \{v \in \mathbb{F} : \hat{f}(0, v) \neq \pm 2^{n/2}\}$

In Lemma 9 there should be $\chi(f(x)) = (-1)^{\mathrm{tr}_1^n(f(x))}$.

p. 13 All functions from Table 1.2 are component–wise plateaued. It can be seen from the fact, that their component are quadratic, and from Lemma 8.

p. 15 The multiset notation used here is $\{*$ value (number of times value is in multiset) $*\}$

p. 16 The proof of $\mathrm{NB}_{x^3} = \{a^3 : a \in \mathbb{F}\}$ is incomplete. In the penultimate paragraph of this section we are interested in solutions of $(az + a^2z^4)$ instead of $x^2(az+a^2z^4)$, and we should indeed have *As* $z = 0$ *is a solution* instead of *As* $x = 0$ *is a solution*, since in the inner sum we are iterating over x. Now it is only proven, that if $a \notin \{b^3 : b \in \mathbb{F}\}$, then $a \in \mathrm{B}_f$. To complete the proof it is needed to consider what happens when a is a cube. Depending on whether the dimension n of the field is odd or even, we have 2, or 4 solution respectively – $z = 0$, and $z \in \{c^3 = 1\}$ (x^3 is either a permutation or a 3–to–1 function). In the odd case the sum reduces to $\chi(0)2^n + \chi(1)2^n = 0 \neq 2^n$, and in the even case we get $\chi(0)2^n + 3\chi(1)2^n = 2^{n+1} \neq 2^n$, therefore these components are not bent, which completes the proof.

p. 18 In Definition 27 the code is called C_f.

p. 19 In Remark 4 there is *for* that should not be there.

p. 20 In the first paragraph there should be *Actually for the code to be a double simplex code, it is only necessary that the APN function is CCZ–equivalent to a permutation.*

pp. 20–21 The theorems Theorem 12 and Theorem 13 are the same theorem – we wanted to recall it in Chapter 2 since it will be used, and made a mistake in numbering the theorems.

p. 22 In the middle of the page, there is a sentence beginning with words *In Section 6.* The verb in the sentence which the sentence should end with is *is given.*

pp. 22–24 It should be noted, that Lemma 14 is also remarked in Section 6 of [2]. In the proof of Lemma 14 the part where we rewrite in matrix form should be presented in a more detailed way.

We can identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ so that $\mathrm{tr}_1^n(uv)$ becomes the scalar product $< u|v >$. Write $\mathrm{tr}_1^n(aA(x)) = 0$ as $< a|A(x) >= 0$ (which is the same as $< a|Ax^T >= 0$). Similarly in the other three cases. Thus $< a|Ax^T + By^T >= 0$ and $< b|Cx^T + Dy^T >= 0$. The scalar product can be interpreted as the matrix multiplication of a row vector and a column vector. The latter two equalities can be thus expressed by a single matrix multiplication

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} Ax^T & By^T \\ Cx^T & Dy^T \end{pmatrix} = 0,$$

which is equivalent to

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0.$$

A matrix that vanishes upon all vectors has to be the zero matrix. Thus

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = 0.$$

Since $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ must be nondegenerate, there has to be $\begin{pmatrix} a & b \end{pmatrix} = 0$, and we get a contradiction. Then it is straightforward, that the argumentation can also be done in reverse, so the condition is really sufficient and necessary.

p. 26 In the first paragraph of the Subsection 3.1.1 the Lemma ? is Lemma 11. The mentioned inequality can then be checked by simply using bound on NB_f and comparing with $|Z_f|$ for the classical Walsh spectrum, which can be found on page 14.

p. 33 In Corollary 2, c is a nonzero element, and U is a space. The proof of Corollary 2 is not correct. But Corollary 2 follows immediately from the fact, that we are considering subspaces of a subset of C.