Errata & addenda in the thesis (English version)

Constanza Riera

March 20, 2006

1 Errata

Chapter 5:

- Page 91, Corollary 5.12: in line -1, it should say "the logarithm (base 2) of the Peak-to-Average Power Ratio of s, $log_2\mathrm{PAR}_{\mathbf{T}}(s)$, is equal to..."
- Page 94, proof of Lemma 5.22: It should start: "$log_2(\mathrm{PAR}_{IH})$ is, as we saw in theorem 5.14, the maximal value of the corank of the modified adjacency matrix over all transforms in $\{I, H\}^n$".
- Page 94, Corollary 5.23: the statement should be: "$\deg(q) = \max |IS|$".
- Page 94, Corollary 5.24: the statement should be: "$\deg(G) = \lambda(G)$".

Chapter 6:

- Page 98, Remark: where it says "$\deg(q(2, y)) = \mathrm{PAR}_{IH}$", it should say "$\deg(q(2, y)) = log_2(\mathrm{PAR}_{IH})$".
- Page 98, Proof of Lemma 6.2: where it says "$\deg(q(2, y)) = \mathrm{PAR}_{IH}$", it should say "$\deg(q(2, y)) = log_2(\mathrm{PAR}_{IH})$"; also, instead of "the degree of $q(1, y)$ is equal to $2^{\max |IS|}$" it should say "the degree of $q(1, y)$ is equal to $\max |IS|$".

Chapter 7:

- Pages 108–110: Proof 2 has some errors. This would be the correct proof:

  Proof: Let $p = x_ix_j + x_i\mathcal{N}_i + x_j\mathcal{N}_j + R$, and $s = (-1)^p$. Let $\mathcal{N}_i = \sum_{r=0}^{\rho} u_r$, and $\mathcal{N}_j = \sum_{t=0}^{\tau} v_t$, (note that they are not necessarily linear). Then, applying theorem 3.7, $N_is = \frac{1+i}{\sqrt{2}} i^{p'}$, where $p' : \mathrm{GF}(2)^n \to \mathbb{Z}_4$, with explicit formula[1]

$$p' = 2\left(p(x) + x_j\sum_{r=0}^{\rho} u_r + \sum_{r\neq s} u_ru_s\right) + 3\left(x_i + x_j + \sum_{r=0}^{\rho} u_i\right). \qquad (1)$$

[1] We denote as $\lambda_0\phi_0 + \lambda_1\phi_1$ or, more generally, as $\sum \lambda_i\phi_i$, with $\lambda_i \in \mathbb{Z}_4$ and ϕ_i Boolean functions, the result of embedding the output of the ϕ_i's into $\mathbb{Z}_4$, multiply them by a scalar $\lambda_i \in \mathbb{Z}_4$, and adding the output mod 4.

Define δ, $\delta_2 \in \{D\}^n$ as $\delta = \frac{\sqrt{2}}{1+i} \prod_{k=i,j} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}_k$. Applying δ to $N_i s$, we get $s' = \delta N_i s = i^{p_i}$, where

$$p_i = 2\left(p(x) + x_j \sum_{r=0}^{\rho} u_r + \sum_{r \neq s} u_r u_s\right) + 3 \sum_{r=0}^{\rho} u_i. \tag{2}$$

This is the result of the action of LC(i). Now we apply LC(j); that is, we first apply N_j to s'. One can see that the result is $N_j s' = \frac{1+i}{\sqrt{2}} i^{p''}$, where $p'' :\ \mathrm{GF}(2)^n \to \mathbb{Z}_4$, with explicit formula

$$\begin{aligned} p'' = 2 \Bigg(& x_i x_j + x_i \sum_{t=0}^{\tau} v_t + x_j \left(\sum_{r=0}^{\rho} u_r + \sum_{t=0}^{\tau} v_t \right) \\ & + \sum_{t \neq u} v_t v_u + \sum_{r,t} u_r v_t + \sum_{r=0}^{\rho} u_r + R \Bigg) \\ & + 3(x_i + x_j + \sum_{t=0}^{\tau} v_t) \end{aligned} \tag{3}$$

Then we apply δ to $N_j s'$ to get $s'' = \delta N_j s' = i^{p_{ij}}$, where

$$\begin{aligned} p_{ij} = 2 \Bigg(& x_i x_j + x_i \sum_{t=0}^{\tau} v_t + x_j \left(\sum_{r=0}^{\rho} u_r + \sum_{t=0}^{\tau} v_t \right) \\ & + \sum_{t \neq u} v_t v_u + \sum_{r,t} u_r v_t + \sum_{r=0}^{\rho} u_r + R \Bigg) + 3 \sum_{t=0}^{\tau} v_t \end{aligned} \tag{4}$$

Now we apply LC(i) again; that is, we first apply N_i to s''. One can see that the result is $N_i s'' = \frac{1+i}{\sqrt{2}} i^{p'''}$, where $p''' :\ \mathrm{GF}(2)^n \to \mathbb{Z}_4$, with explicit formula

$$\begin{aligned} p''' = 2 \Bigg(& x_i x_j + x_i \sum_{t=0}^{\tau} v_t + x_j \sum_{r=0}^{\rho} u_r \\ & + \sum_{r,t} u_r v_t + \sum_{r=0}^{\rho} u_r + \sum_{t=0}^{\tau} v_t + R \Bigg) + 3(x_i + x_j) \end{aligned} \tag{5}$$

Then we apply δ to $N_i s''$ to get $s''' = \delta N_i s'' = (-1)^{p'_{iji}}$, where

$$p'_{iji} = x_i x_j + x_i \sum_{t=0}^{\tau} v_t + x_j \sum_{r=0}^{\rho} u_r + \sum_{r,t} u_r v_t + \sum_{r=0}^{\rho} u_r + \sum_{t=0}^{\tau} v_t + R \tag{6}$$

Define $\delta_2 = -\prod_{k=i,j} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_k$. If we apply now δ_2 to s''', we get

$$p_{iji} = x_i x_j + x_i \sum_{t=0}^{\tau} v_t + x_j \sum_{r=0}^{\rho} u_r + \sum_{r,t} u_r v_t + R, \tag{7}$$

which is by definition 7.2 the formula for pivot on the hypergraph associated to p. Note that this proofs theorem 7.4: Let $d = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, and let $d' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We see that we have applied:

- In position i: $d'dNddN = d' \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} H = H$
- In position j: $\frac{-1}{e^{3\pi i/4}} d'ddNd = (-1)d' \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} H = H$
- Remaining positions: I

$\blacksquare$

Chapter 8:

- In page 117, Corollary 8.4 says that:

$$(N_{j_{t-1}} \cdots N_{j_0})m(-1)^p = \frac{1}{2^{t/2}} \sum_{a \in GF(2)^t} i^{\lfloor (a+1)/2 \rfloor} [m_a](-1)^{p_a + x \cdot a}$$

where $x = (x_{j_0}, \ldots, x_{j_{t-1}})$ and $\lfloor (a+1)/2 \rfloor$ means "the floor function for (a+1)/2".

The correct formula would be

$$(N_{j_{t-1}} \cdots N_{j_0})m(-1)^p = \frac{1}{2^{t/2}} \sum_{a \in GF(2)^t} i^{wt(a)} [m_a](-1)^{p_a + x \cdot a}$$

where $x = (x_{j_0}, \ldots, x_{j_{t-1}})$ and '$wt(a)$' means 'the weight of a as a binary string'.

2 Addenda

- Page 111, proof of theorem 7.7: *Proof:* Let $f \in \mathcal{F}^{n,t}$. Then, it fulfils the condition of definition 7.2 for every edge ij such that $t \leq i, j \leq n$. By section 7.5, pivoting on any of such edges leaves the clique invariant. This means that the number of flat spectra of f will be at least the number of times we can pivot on the clique on the last $n-t$ variables times the number of times we can pivot on the complete bipartite graph $\sum_{i=0}^{t-1} \sum_{j=t}^{n-1} x_i x_j$ (not counting repetitions), plus the identity transform. The number of times we can pivot on the clique of the hypergraph is the same as the number of times we can pivot on a clique of size $n-t$, which is as weel the number of flat spectra of the clique w.r.t. $\{I, H\}^n$. By lemma 4.7, this number is 2^{n-t-1}. Now, we can pivot on each edge of the complete bipartite graph, but note that now the pivoting changes the graph, so a new pivot may not be possible (depending on

$h(x_0, \ldots, x_{t-1})$). Avoiding repetitions, that makes one pivot for every vertex on the first t variables, plus the identity transform. In total, then, we get the lower bound $(t+1)2^{n-t-1}$.

Let $f \in \mathcal{F}^{n,t}$ such that its degree is t. Take $h(x_0, x_1, \ldots, x_{t-1}) = x_0 x_1 \cdots x_{t-1}$. Then, it's easy to see that after doing pivot on any edge mentioned above, the resultant function does not fulfil the condition of definition 7.2. ■

- Page 112, proof of theorem 7.8: *Proof:* Let $f \in \mathcal{F}^{n,t}$. By theorem 7.7, its number of flat spectra w.r.t. $\{I, H\}^n$ is at least $(t+1)2^{n-t-1}$; furthermore, we can see that all the flat spectra correspond to graph operations, so the resulting state is associated to a graph. It can be proven (see [74]) that the graph operation Local Complementation at the vertex j is realised by the application of N_j to the bipolar vector of the function, followed by a diagonal transform, and that implies that the result of applying N_j to the bipolar vector of a function associated to a (simple, non-directed) graph is always flat. On the other hand, the result of applying the identity transform to the bipolar vector of a function associated to a graph is always flat. Therefore, the number of flat spectra of f w.r.t. $\{I, H, N\}^n$ is at least $n+1$ times its number of flat spectra w.r.t. $\{I, H, N\}^n$; i.e. $(n+1)(t+1)2^{n-t-1}$. ■