Corrigendum to "The BMS Algorithm" by S. Sakata, in *Gröbner Bases, Coding, and Cryptography* (eds. M. Sala et.), Springer, 143–163, 2009.

In the descriptions of the BMS algorithm and its variations throughout the paper: S.Sakata, "The BMS Algorithm," pp.143–163,

Page 151, Lemma 2 (2): The formula

$$h := X^{(a-c)-dd'-d} f - \frac{\mathrm{dis}(f)}{\mathrm{dis}(g)} g \in F(a \oplus 1)$$

should be

$$h := X^{d'-d} f - \frac{\mathrm{dis}(f)}{\mathrm{dis}(g)} X^{d'-(a-c)} g \in F(a \oplus 1).$$

Page 152, Algorithm 2, Step 3 (1), line 5: The formula

$$h := X^{\hat{d}-dd'-d} f - d_f g$$

should be

$$h := X^{d'-d} f - d_f X^{d'-(b-c)} g.$$

Page 158, Algorithm 3, Step 3 (1), line 5: The formula

$$h := X^{\hat{d}-dd'-d} f - d_f g$$

should be

$$h := X^{d'-d} f - d_f X^{d'-(b-c)} g.$$

Page 159, Algorithm 4, Step 3 (1), line 5: The formula

$$h := X^{\hat{d}-dd'-d} \mathbf{f} - d_f \mathbf{g}$$

should be

$$h := X^{d'-d} \mathbf{f} - d_{\mathbf{f}} X^{d'-(b-c)} \mathbf{g}.$$

http://www.springer.com/978-3-540-93805-7

Gröbner Bases, Coding, and Cryptography
Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.)
2009, XVI, 430 p., Hardcover
ISBN: 978-3-540-93805-7