Multiplication friendly lifts of (AG) codes over local rings

with R. Cramer & C. Xing, and M. Abspoel & A. Couvreur

Telecom ParisTech

Mar 26, 2019

Motivations

- MPC directly over $\mathbb{Z}/2^k\mathbb{Z}$ is faster than emulated over fields: SPDZ 2^k (Crypto 2018) & Implementation (S&P 2019) 5x faster than SPDZ
- Information theoretically secure MPC requires C with large $d(C^{\perp})$ and $d(C^2)$.

$Good \ lifts$

Elementary properties

Let C be a submodule of \mathbb{R}^n which is a good lift, then we have the following properties:

- (i) if $t \in R$, $z \in R^n$ are such that tz belongs to C, then there exists $c \in C$ such that tz = tc (thus when t is a non-zero divisor: iff $c \in C$);
- (i') the inclusion $\mathfrak{m} C \subset \mathfrak{m} R^n \cap C$ is an equality;
- (ii) any lift in C of any basis of \overline{C} is a basis of C;
- (iii) $d(C) \ge d(\overline{C})$ (equality if R is Artinian, e.g. Galois ring);
- (iv) C^{\perp} is a good lift of \overline{C}^{\perp} (thus is of rank the co-rank of C).

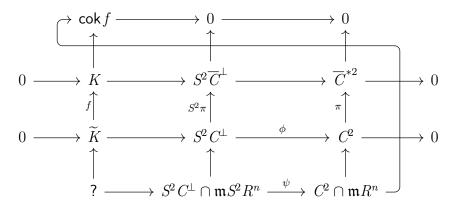
An arbitrary good lift of a code of small square can fail to have its square being a good lift

Ronald's diabolic counterexample

Let \overline{C} and \overline{D} be codes over κ of same dimension and let us assume that dim $\overline{D}^2 < \dim \overline{C}^2$. Let us now build a code E over R and of length equal to the sum of the lengths of \overline{C} and \overline{D} . Let $(\overline{c_i})_i$ and $(\overline{d_i})_i$ be bases of \overline{C} and \overline{D} , let $(c_i)_i$ and $(d_i)_i$ be arbitrary lifts and define Ethe code generated by the vectors $(d_i, pc_i)_i$. Then E is a good lift, because of dimension dim $\overline{D} = \dim \overline{E}$. But E^2 is not a good lift, because of dimension

$$\dim E^2 \geqslant \dim \overline{C}^2 > \dim \overline{D}^2 = \dim \overline{E}^2 \; .$$

Criterion with lift of quadratic forms



Thm: cok f = 0 if and only if C is a good lift

Corollary: If K is a good lift, then C is a good lift. The converse is true if R is a PID or Artinian principal.

$Multiplication\ friendly\ lifts\ of\ AG\ codes$

Thm (uses formal lifts, Walker's codes over artinian rings and Mumford's normal generation)

Let X_0 be a curve of genus g over any finite field \mathbf{F}_{p^r} and $P_0^{(1)}, \ldots, P_0^{(n)}$ distinct rational evaluation points. Consider any divisor D_0 on X_0 with support on rational places, and degree

$$2g+1 \leqslant \mathsf{deg}(D_0) < rac{n}{2}$$
 .

Then the AG codes $C(D_0)$ and $C(2D_0)$ have good lifts C(D) and C(2D) over $R_{\ell}(r)$ (with residue field \mathbf{F}_{p^r}) such that:

$$C(D)^2 = C(2D)$$
. (1)

Linear computation of multiplication friendly lifts

Modulo p^2 : Let C be a good lift in $R_2(r)$.

Then C^2 is also a good lift if and only if there exists a basis $(e_i)_i$ of C, and a set B of unordered couples of indices (k, l) of cardinality dim C^2 , such that the elementary products $(e_k \cdot e_l)_{(k,l) \in B}$ form a basis of C^2 . Namely, if and only if there exists coefficients $\lambda_{i,j,k,l}$ in $R_2(r)$ such that the following equalities in $R_2(r)^n$ hold:

$$\boldsymbol{e_i} \cdot \boldsymbol{e_j} = \sum_{k,l} \lambda_{i,j,k,l} \; \boldsymbol{e_k} \cdot \boldsymbol{e_l} \; \text{ for all } i \leqslant j \; (2)$$

Recursion: let C_ℓ be a good lift in $(\mathbf{Z}/p^l\mathbf{Z})^n$

Then all multiplication friendly lifts —if any— $C_{\ell+1}$ in $R_{\ell+1}(r)^n$ are obtained by solving a linear system of size $O(n^3) \times O(n^3)$. Chuck Norris fact: such lifts always exist for AG codes $/(\mathbb{Z}/p^l\mathbb{Z})$