Code-based cryptography IV

Goppa codes: minimum distance and decoding

Tanja Lange
with some slides by Tung Chou and Christiane Peters

Eindhoven University of Technology

SAC – Post-quantum cryptography

Minimum distance of $\Gamma(L, g)$. Put $s(x) = S(\mathbf{c})$

$$s(x) = \sum_{i=1}^{n} c_i/(x - a_i)$$

Minimum distance of $\Gamma(L, g)$. Put $s(x) = S(\mathbf{c})$

$$
\begin{aligned}
s(x) &= \sum_{i=1}^{n} c_i/(x - a_i) \\
&= \left(\sum_{i=1}^{n} c_i \prod_{j \neq i} (x - a_j) \right) / \prod_{i=1}^{n} (x - a_i) \equiv 0 \bmod g(x).
\end{aligned}
$$

- $g(a_i) \neq 0$ implies $\gcd(x - a_i, g(x)) = 1$,
  so $g(x)$ divides $\sum_{i=1}^{n} c_i \prod_{j \neq i}(x - a_j)$.
- Let $\mathbf{c} \neq 0$ have small weight $\mathrm{wt}(\mathbf{c}) = w \leq t = \deg(g)$.
  For all i with $c_i = 0$, $x - a_i$ appears in every summand.

Minimum distance of $\Gamma(L, g)$. Put $s(x) = S(\mathbf{c})$

$$
\begin{aligned}
s(x) &= \sum_{i=1}^{n} c_i/(x-a_i) \\
&= \left(\sum_{i=1}^{n} c_i \prod_{j\neq i}(x-a_j)\right) / \prod_{i=1}^{n}(x-a_i) \equiv 0 \bmod g(x).
\end{aligned}
$$

- $g(a_i) \neq 0$ implies $\gcd(x-a_i, g(x)) = 1$, so $g(x)$ divides $\sum_{i=1}^{n} c_i \prod_{j\neq i}(x-a_j)$.
- Let $\mathbf{c} \neq 0$ have small weight $\mathrm{wt}(\mathbf{c}) = w \leq t = \deg(g)$. For all i with $c_i = 0$, $x - a_i$ appears in every summand. Cancel out those $x - a_i$ with $c_i = 0$.
- The denominator is now $\prod_{i, c_i \neq 0}(x-a_i)$, of degree w.
- The numerator now has degree $w-1$ and $\deg(g) > w-1$ implies that the numerator is $= 0$ (without reduction mod g), which is a contradiction to $\mathbf{c} \neq 0$, so $\mathrm{wt}(\mathbf{c}) = w \geq t+1$.

Better minimum distance for $\Gamma(L, g)$

- Let $\mathbf{c} \neq 0$ have small weight $\mathrm{wt}(\mathbf{c}) = w$.
- Put $f(x) = \prod_{i=1}^{n}(x - a_i)^{c_i}$ with $c_i \in \{0, 1\}$.
- Then the derivative $f'(x) = \sum_{i=1}^{n} c_i \prod_{j \neq i}(x - a_i)^{c_i}$.
- Thus $s(x) = f'(x)/f(x) \equiv 0 \bmod g(x)$.
- As before this implies $g(x)$ divides the numerator $f'(x)$.
- Note that over $\mathbb{F}_{2^m}$:

$$(f_{2i+1}x^{2i+1})' = f_{2i+1}x^{2i}, \quad (f_{2i}x^{2i})' = 0 \cdot f_{2i}x^{2i-1} = 0,$$

  thus $f'(x)$ contains only terms of even degree and $\deg(f') \leq w - 1$. Assume w odd, thus $\deg(f') = w - 1$.
- Note that over $\mathbb{F}_{2^m}$: $(x+1)^2 = x^2 + 1$

Better minimum distance for $\Gamma(L, g)$

- Let $\mathbf{c} \neq 0$ have small weight $\mathrm{wt}(\mathbf{c}) = w$.
- Put $f(x) = \prod_{i=1}^{n}(x - a_i)^{c_i}$ with $c_i \in \{0, 1\}$.
- Then the derivative $f'(x) = \sum_{i=1}^{n} c_i \prod_{j \neq i}(x - a_i)^{c_i}$.
- Thus $s(x) = f'(x)/f(x) \equiv 0 \bmod g(x)$.
- As before this implies $g(x)$ divides the numerator $f'(x)$.
- Note that over $\mathbb{F}_{2^m}$:

$$(f_{2i+1}x^{2i+1})' = f_{2i+1}x^{2i}, \quad (f_{2i}x^{2i})' = 0 \cdot f_{2i}x^{2i-1} = 0,$$

  thus $f'(x)$ contains only terms of even degree and $\deg(f') \leq w - 1$. Assume w odd, thus $\deg(f') = w - 1$.
- Note that over $\mathbb{F}_{2^m}$: $(x + 1)^2 = x^2 + 1$ and in general

$$f'(x) = \sum_{i=0}^{(w-1)/2} f_{2i+1}x^{2i} = \left(\sum_{i=0}^{(w-1)/2} \sqrt{f_{2i+1}}x^i\right)^2 = F^2(x).$$

- Since $g(x)$ is square-free, $g(x)$ divides $F(x)$, thus $w \geq 2t + 1$.

Decoding of $\mathbf{c} + \mathbf{e}$ in $\Gamma(L, g)$

- Decoding works with polynomial arithmetic.
- Fix $\mathbf{e}$. Let $\sigma(x) = \prod_{i, e_i \neq 0}(x - a_i)$. Same as $f(x)$ before for $\mathbf{c}$.
- $\sigma(x)$ is called error locator polynomial. Given $\sigma(x)$ can factor it to retrieve error positions, $\sigma(a_i) = 0 \Leftrightarrow$ error in i.
- Split into odd and even terms: $\sigma(x) = A^2(x) + xB^2(x)$.
- Note as before $s(x) = \sigma'(x)/\sigma(x)$ and $\sigma'(x) = B^2(x)$.
- Thus

$$
\begin{aligned}
B^2(x) &\equiv \sigma(x)s(x) \equiv (A^2(x) + xB^2(x))s(x) \bmod g(x) \\
B^2(x)(x + 1/s(x)) &\equiv A^2(x) \bmod g(x)
\end{aligned}
$$

- Put $v(x) \equiv \sqrt{x + 1/s(x)} \bmod g(x)$, then $A(x) \equiv B(x)v(x) \bmod g(x)$.
- Can compute $v(x)$ from $s(x)$.
- Use XGCD on v and g, stop part-way when

$$A(x) = B(x)v(x) + h(x)g(x),$$

with $\deg(A) \leq \lfloor t/2 \rfloor, \deg(B) \leq \lfloor (t-1)/2 \rfloor$.