3) MacWilliams Identitäten

(3.1) Def.: Sei G endl. abelsche Gruppe.

$\hat{G} := \{ \chi : G \to \mathbb{C}^* \mid \chi(a+b) = \chi(a) \cdot \chi(b) \quad \forall a, b \in G \}$

$= \operatorname{Hom}(G, \mathbb{C}^*)$ heißt die Charaktergruppe von G

(3.2) Satz (a) $|\hat{G}| = |G|$

(b) $\hat{G}$ bildet ON-Basis des Raums $\mathbb{C}^G$ aller Funktionen $f: G \to \mathbb{C}$ bzgl. dem Skalarprodukt

$$\langle f_1, f_2 \rangle_G := \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)} .$$

Bew: (a) $G = \langle g_1 \rangle \times \ldots \times \langle g_m \rangle$, $d_j := |\langle g_j \rangle|$

$f \in \hat{G}$ eind. best. durch $f(g_j)$ $(j = 1, .., m)$

$f(g_j)$ kann jede bel. d_j-te EW sein

$\Rightarrow \quad |\hat{G}| = d_1 \cdot \ldots \cdot d_m = |G|$.

(b) Vorbem: (i) Nach (a) genügt es ON-Syst. zu zeige. Basis folgt, da $\dim_{\mathbb{C}}(\mathbb{C}^G) = |G|$.

(ii) $f_1, f_2 \in \mathbb{C}^G \Rightarrow \langle f_1, f_2 \rangle_G = \langle f_1 \cdot \overline{f_2}, 1 \rangle$

$(f_1 \cdot \overline{f_2})(g) := f_1(g) \cdot \overline{f_2}(g)$

wo $1 : G \to \mathbb{C}$, $1(g) := 1$.

(iii) $f_1, f_2 \in \hat{G} \Rightarrow f_1 \overline{f_2} \in \hat{G}$ und $f_1 = f_2 \Leftrightarrow f_1 \overline{f_2} = 1$

d.h. genügt zu zeigen:

$$\langle f, 1 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f(g) = \begin{cases} 0 & f \neq 1 \\ 1 & f = 1 \ (\text{klar}) \end{cases}$$

Sei $f \neq 1$, $g_j \in G$ mit $f(g_j) \neq 1$

$G_j := \langle g_1 \rangle \times \ldots \times \langle g_{j-1} \rangle \times \langle g_{j+1} \rangle \times \ldots \times \langle g_m \rangle$

$$\Rightarrow \sum_{g \in G} f(g) = \Big(\underbrace{\sum_{i=0}^{d_j - 1} f(g_j)^i}_{} \Big) \cdot \sum_{g \in G_j} f(g)$$

Vl. von Summe über alle Potenze eines nichttriv. Einheitswurzel also $= 0$.

7

Datum: Betr.:

Bearbeiter:

Blatt: Projekt Nr.: Auftr.Nr.:

(3.3) Def: Sei G endl. ab. Gruppe, $H \leq G$

$$H^{\#} := \{ f \in \hat{G} \mid f(h) = 1 \ \forall h \in H \} \leq \hat{G}$$

heißt die <u>duale Untergruppe</u> zu H.

<u>Klar:</u> $H^{\#} \leq \hat{G}$ und $\hat{G}/_{H^{\#}} \cong \hat{H}$

d.h. $|H| \cdot |H^{\#}| = |G|$

$H^{\#} \cong \widehat{\left(G/_{H}\right)}$

<u>Beisp:</u> $C \leq V$ Code, $\beta \in Bil(V, \mathbb{Q}/_{\mathbb{Z}})$ nichtsingulär

$$\Rightarrow \tilde{\beta} : V \xrightarrow{\sim} V^{*} = Hom(V, \mathbb{Q}/_{\mathbb{Z}}) \cong \hat{V}$$

$v \mapsto (w \mapsto \beta(v,w))$ $\qquad f \mapsto (v \mapsto \exp(2\pi i f(v)))$

Es gilt $\tilde{\beta}(C^{\perp}) = C^{\#}$.

<u>**(3.4) Satz**</u> (Poisson Summation für endl. abelsche Gruppen)

Sei $H \leq G$, G endl. ab. Gruppe, $f : G \to \mathbb{C}$, $g \in G$

$$\Rightarrow \frac{1}{|H|} \sum_{h \in H} f(g+h) = \frac{1}{|G|} \sum_{\chi \in H^{\#}} \hat{f}(\chi) \cdot \chi(g)$$

wo $\hat{f}(\chi) := \sum_{u \in G} f(u) \overline{\chi(u)} = |G| \cdot \langle f, \chi \rangle_G$

<u>Bew:</u> Sei $f' : G/_{H} \to \mathbb{C}$ def. durch $f'(g+H) = \sum_{h \in H} f(g+h)$

$$\Rightarrow f' = \sum_{\chi \in \widehat{(G/_{H})}} \langle f', \chi \rangle_{G/_{H}} \chi$$

$$\langle f', \chi \rangle_{G/_{H}} = \frac{|H|}{|G|} \sum_{\gamma \in G/_{H}} f'(\gamma) \overline{\chi(\gamma)} \underset{\substack{\uparrow \\ \chi \in H^{\#} \text{ auffasse}}}{=} \frac{\overset{|H| \checkmark}{\cancel{|H|}}}{|G|} \sum_{g \in G} f(g) \overline{\chi(g)} \qquad \square$$

1228-96

(3.4) Folg (allgemeine MacWilliams Identität)

Sei $C \leq V$ ein Code, $\beta \in Bil(V, \mathbb{Q}/\mathbb{Z})$ nichtsingulär

$f: V \to \mathbb{C}$ Funktion $\Rightarrow$

$$\sum_{c \in C} f(c) = \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \tilde{f}(c')$$

wo $\tilde{f}(c') = \sum_{v \in V} f(v) \exp(-2\pi i \beta(c', v))$

Bew: (3.3) mit $G = V$, $H = C$, $g = 0$

$$\sum_{c \in C} f(c) = \frac{|C|}{|V|} \sum_{\chi \in C^\#} \hat{f}(\chi) \cdot \underbrace{\chi(0)}_{=1}$$

$$\hat{f}(\chi) = \sum_{v \in V} f(v) \overline{\chi(v)} = \tilde{f}(c')$$

wo $c' \in C^\perp$ dadurch def. ist, daß $\chi(v) = \exp(2\pi i \beta(c', v))\ \forall v \in V$. $\rfloor$

(3.5) Folg (MacWilliams Identität für Hamming Gewichtszähler)

Sei V abelsche Gruppe

$C \leq V^N$ ~~Code~~ Ugr, $\beta: V \times V \to \mathbb{Q}/\mathbb{Z}$ nichtsingulär

$$hwe(C)(x,y) = \frac{1}{|C^\perp|} hwe(C^\perp)(x + (|V|-1)y, x-y)$$

Bew: Seien $x_0, y_0 \in \mathbb{C}$ beliebig

$$f(v) := x_0^{N-wt(v)} y_0^{wt(v)} \quad \forall v \in V^N$$

$$\Rightarrow \sum_{c \in C} f(c) = hwe(C)(x_0, y_0) \underset{(3.4)}{=} \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \tilde{f}(c')$$

$$\tilde{f}(c') = \sum_{w \in V^N} \underbrace{\exp\left(-2\pi i \sum_{j=1}^N \beta(c'_j, w_j)\right)}_{\prod_{j=1}^N \exp(-2\pi i \beta(c'_j, w_j))} \underbrace{x_0^{N-wt(w)} y_0^{wt(w)}}_{\prod_{j=1}^N x_0^{1-wt(w_j)} y_0^{wt(w_j)}}$$

8

Datum: Betr.:

Bearbeiter:

Blatt: Projekt Nr.: Auftr.Nr.:

$$= \sum_{w \in V^N} \prod_{j=1}^{N} \exp(-2\pi i \beta(c_j', w_j)) \, x_0^{1-wt(w_j)} \, y_0^{wt(w_j)}$$

$$= \prod_{j=1}^{N} \left(\left(\sum_{\substack{a \in V \\ a \neq 0}} \exp(-2\pi i \beta(c_j', a)) \cdot y_0 \right) + x_0 \right)$$

Sei

$$q(c_j') := \sum_{0 \neq a \in V} \exp(-2\pi i \beta(c_j', a))$$

$$c_j' = 0 \Rightarrow q(c_j') = |V| - 1$$

<u>Beh</u>: $c_j' \neq 0 \Rightarrow q(c_j') = -1$.

Sei für $b \in V$ $\chi_b : V \to \mathbb{C}^*$, $a \mapsto \exp(-2\pi i \beta(b,a))$ $\Rightarrow \chi_b \in \hat{V}$

$b \neq 0 \Rightarrow \chi_b \neq 1$

$$\Rightarrow \langle \chi_b, 1 \rangle = \frac{1}{|V|} \sum_{a \in V} \exp(-2\pi i \beta(b,a)) = 0$$

$$\Rightarrow \sum_{\substack{a \in V \\ a \neq 0}} \exp(-2\pi i \beta(b,a)) = -\exp(-2\pi i \beta(b,0)) = -1$$

also

$$hwe(C)(x_0, y_0) = \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \hat{f}(c')$$

$$= \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} \prod_{j=1}^{N} (q(c_j') \cdot y_0 + x_0)$$

$$= \frac{1}{|C^\perp|} \sum_{c' \in C^\perp} (x_0 - y_0)^{wt(c')} \cdot ((|V|-1) y_0 + x_0)^{N - wt(c')}$$

$$= \frac{1}{|C^\perp|} hwe(C^\perp)\left(x_0 + (|V|-1) y_0, \; x_0 - y_0 \right).$$

1228-96

(3.6) Def: Sei $C \leq V^N$ ein Code.

(a) $\mathbb{C}[V^N]$ = Gruppenring der abelschen Gruppe V^N

$\cong (V^N)^{\mathbb{C}}$ als $\mathbb{C}$-VR.

$\mathbb{C}$-Basis $(e_v \mid v \in V^N)$

(b) Der <u>volle Gewichtszähler</u> von C ist

$$\mathrm{fwe}(C) = \sum_{c \in C} e_c \in \mathbb{C}[V^N].$$

(3.7) Bem:
$$\mathbb{C}[V^N] \to \mathbb{C}[x_v \mid v \in V]$$
$$e_{(v_1, \dots, v_N)} \mapsto x_{v_1} \cdots x_{v_N}$$
bildet $\mathrm{fwe}(C)$ auf $\mathrm{cwe}(C)$ ab.

(3.8) Folg (MacWilliams Identität für volle Gewichtszähler)
Sei $C \leq V$ code, $\beta \in \mathrm{Bil}(V, \mathbb{Q}/\mathbb{Z})$ n.s.
$$\mathrm{fwe}(C^\perp) = \frac{1}{|C|} \sum_{w \in V} \sum_{v \in C} \exp(2\pi i\, \beta(v,w))\, e_w$$

Bew: Sei $w \in V \Rightarrow$
$$\sum_{v \in C} \exp(2\pi i\, \beta(w,v)) = \begin{cases} |C| & \text{falls } w \in C^\perp \\ 0 & \text{sonst} \end{cases}$$
$$= |C| \cdot \langle \chi_w, 1 \rangle$$
$$\chi_w : v \mapsto \exp(2\pi i\, \beta(w,v)) \in \hat{V}. \quad \lrcorner$$

(3.9) Folg (MacWilliams Id. für vollst. Gew.zähler)
$C \leq V^N$ Code, $\beta \in \mathrm{Bil}(V, \mathbb{Q}/\mathbb{Z})$ n.s.
$$\mathrm{cwe}(C^\perp) = \frac{1}{|C|} \cancel{\sum_{v \in C}} \cancel{\sum_{w \in}} \mathrm{cwe}(C)(y_v)$$
$$\text{wo } y_v = \sum_{w \in V} \exp(2\pi i\, \beta(v,w))\, x_w$$

Do 12.5. / Do 2.6.